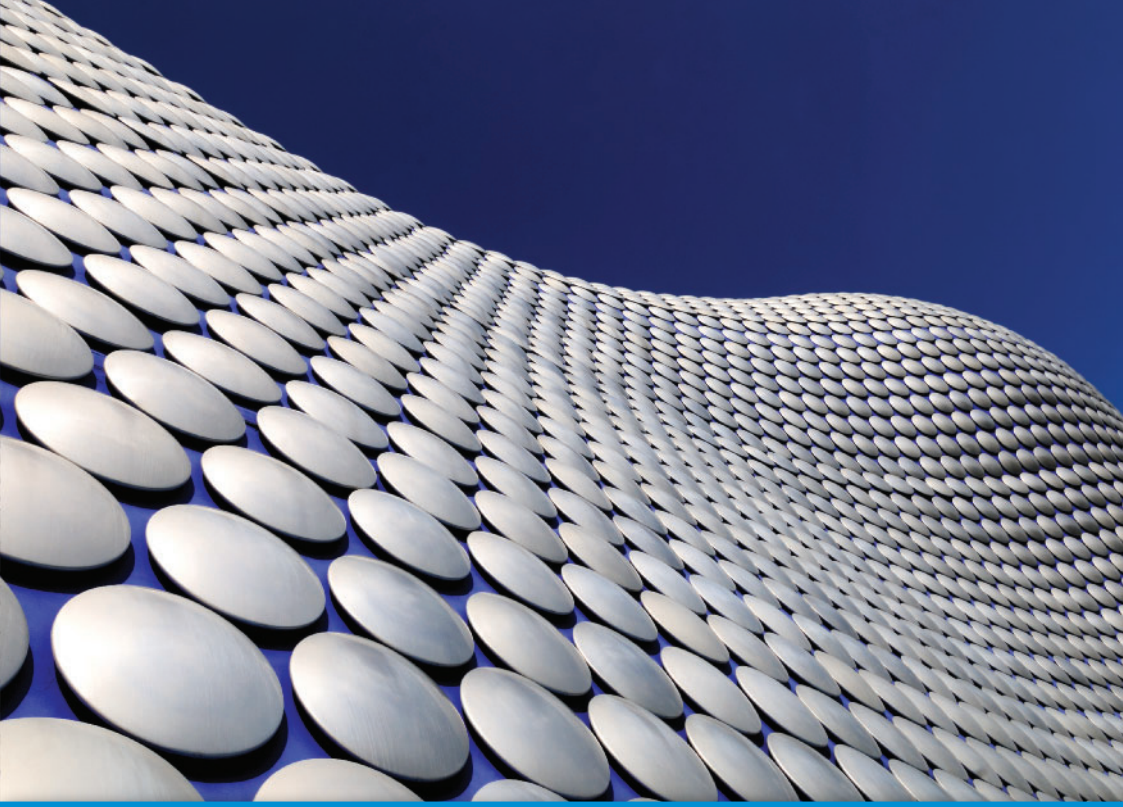

MIDLANDS FRAUD FORUM

Bringing the public & private sectors together

A GUIDE TO KEEPING YOU SAFE AND SECURE FROM FRAUD

IN TODAY'S PERSONAL AND BUSINESS WORLD

Brought to you by the **Midlands Fraud Forum**

MIDLANDS FRAUD FORUM

COMBATTING FRAUD

in association with

Ministry of JUSTICE

Home Office

National Fraud Authority

British Chambers of Commerce
150 years of helping business | 1860-2010

BIS Department for Business Innovation & Skills

The messages within this booklet are based on anti-fraud and police crime prevention advice.

The Midlands Fraud Forum (MFF) supports the National Fraud Authority and 'Action Fraud'.

We are targeting not just small and medium businesses across the East and West Midlands, but the people both inside and outside those businesses.

Fraud can happen to anyone, at any level, so read on and find out how you can protect yourself and your business.

BUSINESSES – HOW YOU CAN PROTECT YOURSELF

86%
OF FRAUDSTERS ARE MANAGERS

www.midlandsfraudforum.co.uk

WHAT DOES A FRAUDSTER LOOK LIKE?

The typical company fraudster is a trusted male executive who gets away with over 20 fraudulent acts over a period of up to five years or more.

If you have someone of this description and trust him to work with access to finances and the minimum of supervision, think long and hard about what to do next! Board members of companies (directors) commit nearly a fifth of all fraud.

PREVENTION

(such as introducing ethics and integrity measures at the top management level)

WILL ALWAYS BE MORE EFFICIENT AND COST-EFFECTIVE

The patterns concerning insider fraudsters are similar right across geographical regions.

- 85 percent of fraudsters are male.
- The typical fraudster is aged between 36 and 45.
- By the time he starts enriching himself by illegal means, he has usually been employed by the company for six or more years.
- He typically works in the finance department and commits the fraud single-handed.
- In 86 percent of cases he is at management level - and in two thirds of cases he is a member of senior management.
- Greed and opportunity are his motivating factors.

The financial damage inflicted by fraudsters can be severe. In most cases, the affected companies have to bear the losses themselves and in many cases this will lead to ruin, not just of finances but to reputation.

HOW YOUR BUSINESS CAN COMBAT 'INSIDER FRAUD'

- Have a clear policy and procedure on your organisations approach to fraud issues.
- Adopt a zero-tolerance policy towards all cases of staff fraud.
- Introduce clear guidelines for staff on the minimum standards of behaviour expected.
- Provide fraud awareness training to staff.
- Carry out thorough vetting of all new staff before they take up employment.
- Restrict staff access to information systems according to the needs of their individual role.
- Regularly review financial systems and processes with particular regard to authorisation thresholds and segregation of duties.
- Be wary of suppliers/contractors who insist on dealing with just one individual.
- Periodically review business procedures and controls for exposure to fraud.
- Ensure your business premises have adequate physical security.

RESTRICT STAFF ACCESS

And it's not just from inside the company that the attack may come...

HOW YOUR BUSINESS CAN COMBAT 'CARD NOT PRESENT' FRAUD

- Discuss with your bank the use of a secure payment system (such as Verified by Visa and MasterCard SecureCode).
- Make use of the Address Verification Service (AVS) and Card Security Code (CSC).
- Consider using intelligent fraud detection software provided by third parties.
- Always be mindful that payment authorisation does not guarantee payment.
- Call the customer to verify the transaction details.
- Be wary of suspicious delivery addresses.
- Proceed with care when processing priority shipments for fraud-prone merchandise such as TVs or mobile phones, electrical and white goods.
- Exercise caution when dealing with transactions from abroad.
- Be alert to changes in a customer's usual purchasing patterns and order volumes.
- Consider using secure courier delivery for high value products.
- Where possible, do not proceed cardholder not present transactions and then allow the customer to collect the goods without seeing the card.

HOW TO PROTECT YOUR BUSINESS

FROM E-CRIME

Attacking computer systems (e-crime) can be devastating to anyone, but in particular to small and medium enterprises. Awareness of the risks and recognising that simple measures, some of them at no cost, are the first step in beating these fraudsters.

IF YOU GET A BUSINESS OFFER WHICH SOUNDS GOOD, DON'T TAKE IT FOR GRANTED

YOU GET NOTHING FOR NOTHING!

www.midlandsfraudforum.co.uk

Hackers will exploit any weakness and vulnerability in the system and can destroy the reputation of a business, alter or empty the accounts and even close the company down.

In the same way they can assume an individual's identity and create havoc when they obtain details of credit cards, online banking and saving accounts.

There are many systems that are available for free from the Internet but these are possibly better suited for use in people's houses. Businesses may feel more secure with a comprehensive package that includes anti-virus, anti-spam, firewall, spyware and malware detection, removal with automatic scanning and updating.

- Any employees linked into the business network must also have the same level of protection.
- Use a password at least eight characters long and utilise a combination of different cases, numbers and characters.
- Passwords allow a system to be accessed so do not reveal them to anyone, either inside or outside the office.
- Try not to use the names of family, pets or business as hackers may be able to identify your password with very little research.
- Don't record your passwords or access codes in places near your computer where a hacker could access them.
- Be careful when opening e-mails and attachments.

E-mails are often used to carry viruses such as Trojans and worms which will infect computer systems. These devices can be set up to record what keyboard activity takes place so that when you use online banking your details are passed on without your knowledge and your accounts are then accessed by the offender.

'Phishing' e-mails pretend to be from somebody you trust, such as a bank or other financial institution and can look identical to the genuine organisation. Typically, the e-mail would request the account holder to log onto a bogus website which looks like the original and then request the account holder to confirm their username and password. Others will ask for the security code or pin number.

INSTALL

AN ANTI-VIRUS, A FIREWALL AND ANTI-SPYWARE ON ALL COMPUTER SYSTEMS

Educate staff

Include fraud prevention and detection in induction program. Provide on-going fraud training.

Make sure all employees are aware of their responsibilities and what the company policy is in relation to security. Train them in awareness concerning the opening of e-mails and attachments.

Operate a clear desk policy

It is vital that staff know the implications of losing a laptop or what can happen when confidential company information is lost or stolen.

HOW TO PROTECT YOURSELF FROM FRAUD WITHIN BUSINESS (ACCOUNTING FRAUD)

Accounting fraud; when an employee or organisation presents accounts that do not reflect the true value of financial activities, either over or understating liabilities.

Are you a victim?

It can be tricky to discover acts of falsifying accounts, particularly if you are managing an organisation.

At one end of the scale false accounting could be someone inflating their expenses, at the extreme end of the scale the fraud may mean that a company has serious financial losses and is trading while insolvent such as in the headline grabbing Enron case.

What should you do?

Report the fraud directly to Action Fraud, regardless of the money involved. From here the case may be referred to the police for further investigation.

You will need to determine the nature and extent of any losses; this can be done by accountants inside or outsourced to consultants.

- Vet employee's CVs and references thoroughly.
- Control access to buildings and systems using unique identification and passwords.
- Restrict and closely monitor access to sensitive information.
- Impose clear segregation of duties.
- Consider job rotation.
- Use tiered authority and signature levels for payments.
- Periodically audit processes and procedures.
- Promote a culture of fraud awareness among staff.
- Adopt and rigorously implement a zero tolerance policy towards employee fraud.
- Have a clear response plan in place in case fraud is discovered.

Here are simple steps you can take to protect yourself against fraud.

- Do not give any personal information (name, address, bank details, e-mail or phone) to organisations or people before verifying their credentials.
- Always properly verify references.
- When you are online take steps to ensure that the person you are communicating with is who they say they are.
- If an offer seems too good to be true – it probably is.
- If you get a business offer which sounds good, don't take it for granted, check out the authenticity of the organisation through regulatory bodies.

COMPANY TAKEOVER FRAUD

Check your business registered details at Companies House on a regular basis. Register for Companies House PROOF scheme, and monitor service.

Review your credit status on a regular basis.

PEOPLE – HOW TO BE SECURE

AND FEEL MORE SECURE

HOW TO PROTECT YOURSELF AGAINST BANK CARD AND CHEQUE FRAUD, OFF OR ONLINE.

Don't let criminals steal your cards or cheque book and gain access to funds in your account.

KEEP YOUR BANK'S 24 HOUR NUMBER ON YOU AT ALL TIMES

www.midlandsfraudforum.co.uk

Are you a victim?

Your cards or cheque book have been stolen or faked and you notice unfamiliar transactions on your statement or find out that your overdraft limit is suddenly exceeded.

What should you do?

- Immediately phone your bank on its 24 hour emergency number and stop the cards.
- Contact www.actionfraud.org.uk to get advice and guidance.
- Keep a record of all communications.
- Get a copy of your personal credit report from one of the credit reference agencies, Call Credit, Equifax or Experian.

Consider contacting CIFAS the UK's Fraud Prevention Service.

How to prevent this type of fraud?

- Keep your cards and their details safe at all times. Don't let your card out of your sight when you do a transaction.
- Store safely financial documents and shred them when getting rid of them.
- Sign any new cards as soon as they arrive.
- Cut expired cards through the magnetic strip and chip when replacement cards arrive.
- Don't write your pin number down anywhere and ensure that you are the only person who knows it.
- Don't let people see you entering your pin by shielding the number when you type it in. If you think someone has seen you then phone your bank to change it.
- If you spot anything unusual about the ATM machine, report it immediately.
- If someone is making you feel uncomfortable cancel the transaction and use a different machine.
- Destroy or preferably shred receipts from the cash machine, mini-statement or balance enquiry when you dispose of them.

ONLINE BANKING

Make sure your computer has up-to-date anti-virus software and a firewall installed. Consider using anti-spyware software.

When banking online there should be a locked padlock or unbroken key symbol in your browser.

Be very wary of unsolicited e-mails, "phishing" e-mails requesting personal financial information. Your bank or police would never ask you to disclose your PIN.

Ensure your browser is set to the highest level of security notification and monitoring. The safety options are not always activated by default when you install your computer.

Always access Internet banking sites by typing the bank's address into your web browser. Never go to a website from a link in an e-mail and then enter personal details.

Never reply to requests for money, no matter how tempting or deserving the cause sounds, without checking it is genuine.

ONLINE SHOPPING

Sign up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online. This involves you registering a password with your card company.

Only ever shop on secure sites. Before submitting card details ensure the locked or unbroken key symbol is showing in your browser. The retailer's Internet address will change from "http" to "https" when a connection is secure.

Use only secure and trusted websites.

Never send your PIN over the Internet.

Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address and phone number.

The guidance is taken from Personal Security Plan 2008 – "The best ways to minimise your chances of becoming a victim of fraud."

www.banksafeonline.org.uk/documents/Personal_Security_Plan_2007.pdf

COUNTERFEIT CHEQUE FRAUDS

These rely on your willingness to help someone else and perhaps make a profit.

Are you a victim?

You've advertised an item for sale and someone has contacted you saying they want to buy it. They send you a cheque into your bank account and ask that you withdraw the excess in cash and send it to them via money transfer.

After the money has gone from your account, the bank identifies the cheque as a fake and debits money to the value of the cheque out of the account, leaving you out of pocket.

From November 2007, the banking industry changed the way cheques are processed to benefit customers accepting cheques. It means that for the first time you can be sure that after a maximum of six working days (after paying in a cheque) the money is yours and you are protected from any loss should the cheque turn out to be fraudulent. This means that the funds from a cheque cannot then be reclaimed without your permission, unless you are a knowing party to fraud.

Despite this positive change the banking industry continues to recommend that you should be wary of accepting cheques or bankers' drafts if you don't know or trust the person offering them to you – particularly if they are of high value.

If you believe you may have become a victim of crime, keep any documents, letters or e-mails sent by the fraudster as possible evidence.

How to prevent?

Beware of overseas buyers who readily agree a price without seeing what they are buying.

If the buyer refuses to agree shipping costs it indicates a fraud.

Any buyer who sends a cheque for more than the agreed amount and asks you to send cash to balance it is most likely a fraudster.

Always use a trusted payment mechanism like 'Paypal'. Do not be forced to deviate away from your tried and trusted method of Internet payment.

IDENTITY FRAUD

ONE OF THE UK'S
FASTEST GROWING CRIMES

Identity Fraud; when someone else steals your personal identity, and, or financial information, to use it to purchase goods, services and access facilities in your name.

Remove your name from unwanted mailing lists. Arrange for mail to be redirected if you move address, and notify any relevant organisations.

If you don't receive any mail, check with Royal Mail that a redirection has not been set up in your name without your knowledge.

Limit the number of personal documents you carry with you, carry only those that you need. Leave the rest securely at home.

MORE ON THE MIDLANDS FRAUD FORUM...

Effective fraud prevention requires us to be open about our experiences and share our knowledge. Recent changes in the Government's approach to fraud have started a culture change, particularly with regards to private individuals but much work is still required in the corporate sector. In common with the other fraud fora across the country, a key aim of this website is to encourage and participate in this knowledge sharing.

MEMBERSHIP

The key benefit of membership is becoming part of a valuable network of people directly involved in the business of combating fraud every day. The opportunity to share knowledge, experiences and best practices is an essential business requirement in today's public and private sectors.

Members of the MFF will be kept informed of all conferences, master classes and specialist forums. In addition they will be offered special discounted rates for these events. As this is a non-profit organisation membership fees are kept to a minimum, currently being £50 per person per annum.

If you have any questions about membership please visit www.midlandsfraudforum.co.uk

ANNUAL CONFERENCE

Each year the MFF holds a conference for all its members, usually held in February. We invite speakers from across industry and the public sector to talk about current fraud-related issues. Furthermore there are a series of optional workshops and discussion groups. All of these are designed to be directly relevant to people involved in combating fraud and fraudulent behaviour in the workplace.

HOW TO APPLY

Membership of the Midlands Fraud Forum for the remainder of the calendar year is included in the fee to attend a Midlands Fraud Forum event. You may apply to attend an event via our Events page on the website.

If you wish to become a member but are unable to (or do not wish to) attend an event then please visit www.midlandsfraudforum.co.uk

action fraud
actionfraud.org.uk

REPORT A FRAUD TO THE
NATIONAL FRAUD REPORTING CENTRE
at www.actionfraud.org.uk

Other useful links

www.cifas.org.uk
The UK's fraud prevention service

www.companieshouse.gov.uk
Information on companies and directors

www.ukpayments.org.uk
A one-stop shop for information on making a payment in the UK

www.attorneygeneral.gov.uk/nfa
The latest news from the National Fraud Authority and the wider counter-fraud community

If you have any comments on the content of this booklet please contact Glenn Wicks:
Tel: 0115 9351170 Email: Glenn.Wicks@bis.gsi.gov.uk

BECOME A MEMBER, VISIT www.**midlandsfraudforum**.co.uk

OUR MISSION STATEMENT

The aim of the MFF is to provide an industry led initiative involving public and private sectors to reduce fraud by:

- Increasing awareness of fraud
- Communicating the risk
- Promoting best practice in countering fraud

How will we do this?

We will fulfil our mission statement through the development and delivery of:

- Education strategy
- Media strategy
- Funding strategy
- Networking/membership structure

Designed and produced by ClashDesign.co.uk