THE LITTLE BOOK OF BIG SCAMS

BUSINESS EDITION

METROPOLITAN POLICE

TOTAL POLICING

NEW SCOTLAND YARD

BIG SCAMS

The Little Book of Big Scams offers fraud prevention advice to safeguard your business against fraudulent acts whilst complying with the law and relevant regulations. This advice is for small and medium enterprises but is as relevant to individuals as to larger organisations.

We are living in an age of mobile technology and wireless communications that is both easily accessible and affordable. The worldwide web has provided consumers with an unprecedented opportunity to shop, bank and conduct an array of other financial activities on line, but for fraudsters ,this is a growth industry too!

Criminals have identified that there are rewards to be reaped from online fraud; however, there are simple steps that you can take to stop them. Read this free booklet and follow the 10 top tips to discover just what is needed to defend yourself and your business against fraud and... put the criminals out of business!

Simon Letchford
Detective Chief Superintendent

THE LITTLE BOOK OF BIG SCAMS
BUSINESS EDITION

CONTENTS

BIG SCAMS

INTRODUCTION

The Metropolitan Police Service's Operation Sterling is pleased to bring you a new version of The Little Book of Big Scams. This version has been designed specifically to protect small and medium enterprises (SMEs), which account for 99% of all UK businesses and employ over 13 million people. These businesses range from the 'micro' business, employing 1 or 2 people, through to 'medium' sized businesses employing up to a few hundred.

SMEs can be found everywhere; on the high street, online, at home and in villages, towns and cities. **They are vital to the overall success of the British economy**. There are many threats against them, not least of which is the threat of fraud on a day-to-day basis.

Fraud is simply the intent or the act of misrepresentation to cause a gain or loss.

With limited resources and turbulent economic conditions, SMEs typically prioritise innovation, growth and survival over due diligence, internet controls and risk mitigation; these can often seem expensive, burdensome and bureaucratic business practices. However, this approach leaves SMEs particularly vulnerable to fraud with many SME owners and managers unaware of the fraud risks their business faces.

The impact of fraud is often more dramatic in SMEs which simply cannot afford the losses that may arise. Often, these losses can result in business failure.

The threat of fraud is very real. The National Threat Assessment puts fraud on a par with drugs and terrorism. 37% of organised criminal networks commit fraud which in turn is used to fund other crime.

It is important to recognise that a fraud can come from anywhere; internal staff, customers, suppliers as well as unconnected third parties. Fraud can also seem inherently complicated and difficult to understand as criminals use a range of tools and techniques at their disposal.

Whilst we cannot provide a single solution to prevent all fraud, this booklet seeks to explain some of the more common frauds that are a threat to SMEs and provides simple advice that if followed, can help an SME to identify and take action to protect themselves.

This booklet builds on the success of The Little Book of Big Scams published in 2012 aimed at consumers. Whether you have already set up a business or are looking to start a new venture, it will enable you to have a better understanding of fraud threats and prevention. Awareness of these threats and prevention tools is key. We have incorporated some case studies along with best practice and advice. Please read this booklet. It could be the difference that ensures your business continues to thrive.

REMEMBER:
FRAUD CAN COME FROM ANYWHERE; INTERNAL STAFF, CUSTOMERS, SUPPLIERS AS WELL AS UNCONNECTED THIRD PARTIES.

BIG SCAMS

TEN TOP TIPS TO HELP YOU FIGHT FRAUD

1 Be sceptical

If it sounds too good to be true, it probably is. Always approach deals, opportunities, documents, transactions and information with an inquiring and questioning mind.

2 Know your business inside out

Having a thorough understanding of your business will ensure that you know:

- how it operates.
- the staff you employ.
- the products and services it provides.
- your target market and your business obligations, both legally and regulatory.

This will help you detect when something is not right.

3 Know your customers and suppliers

Understanding who you do business with will help identify occasions where a seemingly ordinary business request or transaction looks out of the ordinary for that customer or supplier and may potentially be fraudulent. Conduct due diligence using a risk based approach. e.g. verify legitimacy of customer/supplier details you have stored on file as well as online searches.

4 Identify areas where your business is vulnerable to fraud

Take some time to imagine how a fraudster might target your business, internally and externally and consider testing the systems you have put in place to reduce your risk. Ensure you and your staff are familiar with those systems and review them on a regular basis.

5 Develop a strategy and talk about fraud

Consider a prevention strategy detailing controls and procedures to prevent and detect fraud that is adequate and appropriate for your business. Staff will look to owners and managers for guidance as to what behaviour is acceptable. Talk about fraud with your staff, suppliers and other contacts. Your staff need to understand the risks and the impact of any losses on the business and to themselves.

6 Take extra care with all things cyber

With increasing threats from cybercrime make sure your business technology is adequately protected against attacks. Make sure you back up your systems in case they go wrong.

7 Understand your finances

Understand how money leaves your business e.g. methods of payment, who has authority to make those payments and who checks that those payments are legitimate. Always check your bank statements!

8 Secure and protect your property

Including laptops, computers, smartphones and intellectual property and consider factoring in business insurance to cover these items if they are compromised or stolen. Use and maintain inventories.

9 Develop an action plan

Consider where you might need professional or legal advice. While prevention is better than cure, it is important for you and your business to be prepared for the worst. Having an action plan in place will help limit your losses to fraud and help to ensure your business doesn't suffer damaging losses.

10 Always report fraud and get help

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded. They provide a central point of contact for information about fraud and financially motivated internet crime Report online at actionfraud.police.uk or by telephone on 0300 123 2040.
Report to the police in your area if the suspect is known to you or still in the vicinity.

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

BIG SCAMS

MYTH BUSTERS

1 If a business is registered with Companies House it must be legitimate.

FALSE!

Companies House is a registrar of companies which incorporates and registers companies in the UK. It does not act as a regulator and does not verify the legitimacy of company operations.

2 My business has an audit so I am free from fraud.

FALSE!

Auditors are responsible for ensuring that financial statements are a reasonable reflection of the financial performance and position of the business they audit. It is not their responsibility to detect fraud; this is the responsibility of the businesses' management.

3 I run a legitimate business. I don't have to worry about money laundering.

FALSE!

Many SMEs are subject to money laundering regulations, including money service businesses, virtual offices and those registered with and regulated by the Financial Conduct Authority. Before setting up a business know where you stand in relation to money laundering regulations, registration etc. Money laundering regulations have been put in place to protect the UK financial system and thereby place certain obligations on businesses most at risk, including suspicious activity reporting.

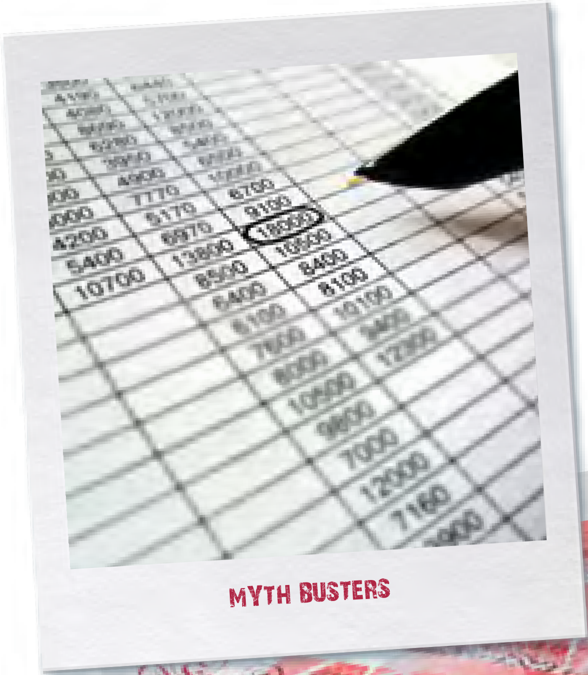
Even if your business is not covered by these regulations it is best practice to familiarise yourself with them to ensure that your business does not fall victim to criminal schemes to 'clean' dirty money.

You should be aware that if your business receives money which represents proceeds of crime, it may be required to return those funds thereby creating a loss to the business.

4 It does not matter if my employee used my business to conduct fraud; I didn't know and I am innocent.

FALSE!

If an employee or manager is able to use your business to carry out fraud against third parties, customers or suppliers, it is possible that the business may be held accountable. There is also a risk that you could be held personally accountable if you did not put in place appropriate controls and procedures to prevent fraud.



BIG SCAMS

IT CAN HAPPEN TO YOU!

A company's accounts section became suspicious of a payment to a contractor who had previously worked for them but had not invoiced the company for over a year.

The accounts section discovered the anomaly when they were changing their systems over to a new secure programme. A number of purchase order accounts needed to be migrated across that still had funds in them. These accounts needed to be reviewed to see whether they should remain open or whether the work had been completed and the accounts should be closed.

A senior member of staff was overseeing this process and it transpired that a payment of **£31,960** had been made to a contractor who had not worked for the company for over a year. Further investigation revealed that associated invoices contained different banking details to previous invoices from the contractor. User profiles used to change the banking details and the recipients of the payments were linked back to two members of staff within the company.

Internal enquiries prompted one staff member to give an explanation; they had been testing the new internal banking systems using one of their own personal bank accounts. This was mistakenly done on the live system instead of a test environment. The staff member was instructed to pay back the funds which he did. However, later checks conducted on the bank account revealed that a further **£25,000** had been transferred from the company into the member of staff's bank account.

This was reported to the police and the staff member was arrested. He admitted to transferring both payments into his own personal account and spending £25,000 of the company's money. He was sentenced at court to 12 months imprisonment and ordered to repay the £25,000 plus costs.

This is known as insider fraud; where an individual within a company uses their inside influence or position of trust to commit fraud.

SCAM

BIG SCAMS

CURRENT FRAUD TRENDS

In its Annual Fraud Indicator for 2013, the National Fraud Authority estimated that fraud cost SMEs £9.2 billion that year. It found that more than 1 in 4 of the businesses it surveyed had been victims of fraud in the last financial year and that the most common fraud types were:

- ⚠ Payment/banking fraud (69%)
- ⚠ Accounting fraud (26%)
- ⚠ Procurement fraud (21%)

86% of businesses suffered fraud from external sources and 56% of businesses suffered fraud internally.

Overall, 40% of businesses surveyed suffer both internal and external fraud and more than one third of them suffer cyber enabled fraud.

Whilst a monetary loss could potentially devastate a business, it is important also to not underestimate the impact of reputational damage. Brand damage could result in much greater losses than the actual amount lost to the fraud itself.

BIG SCAMS

FRAUD PREVENTION

SMEs face a particular difficulty in balancing their fraud prevention activities with the resources they have available (both money and time).

It is vital that SMEs do not put profitability at risk by implementing unnecessary and needlessly expensive 'gold standard' fraud control systems. We suggest a basic, pragmatic, practical approach.

- ⚠ Proportionality is key. Make sure the actions you take are appropriate to your business type and size.
- ⚠ A good starting point is to understand where your business is most at risk of fraud. Conduct a review of your business functions and processes and consider how a fraudster may seek to exploit weaknesses.
- ⚠ Next, develop systems and processes to reduce those identified risks. Focus on closing those gaps which if targeted by a fraudster could cause the biggest damage to your business.
- ⚠ Communicate those systems and procedures to staff and if appropriate, to customers and suppliers too.
- ⚠ Make sure the right person in the business is giving the 'fraud prevention' message in the right way to ensure that it is heard.
- ⚠ Create a fraud prevention culture. Talk about fraud. Fraud prevention is not a one off activity. Regularly and routinely review your functions to ensure that systems and processes are relevant, effective, adhered to and improved where necessary.
- ⚠ Contingency planning; discovering a fraud can lead to a chain of events that can be incredibly disruptive, damaging, stressful and costly. It is important that you, your business and your staff are aware of what needs to happen when a fraud is suspected or discovered and effective planning will help the business to recover as quickly as possible.

FRAUD STRATEGY

Ideally, every business should have a clearly defined fraud prevention strategy that incorporates all of the elements contained in the diagram shown, starting with a written fraud policy.

Policy

Having protocols and policies in place for dealing with fraud will help you establish a good grounding for identifying it and minimising your risk of becoming a victim. The policy should be simple and easy to read.

You should emphasise a zero-tolerance approach to criminal breaches of your policies and the law surrounding it.

You also need to express the possibility of any breaches being investigated by the police or other designated authorities.

You may also want to make it clear to your members of staff – however big or small your business is – they also have a responsibility to detect and prevent fraud. This should be promoted to all members of staff whatever their status or role.

Prevent and Detect

In order to detect fraud you need to have effective systems and processes in place covering all aspects of your business.

Consider regular, routine planned audits. Conduct irregular unplanned audits (i.e. where the staff and areas of your business are not given prior notification).

Have a separate "whistle blowing" policy so that members of staff know exactly who to report any concerns and suspicions to, how they should do it and what levels of protection they can expect.

This policy should be promoted wherever possible.

Investigate

Once you have identified a fraud you will need to formulate a clear strategy to deal with it. The first thing to consider is the extent of the fraud. Do not assume you have identified the full extent straight away. For example, if it is one member of staff that is suspected, consider other staff members they work with. Consider whether you should take action straight away or monitor and investigate further. If you investigate further, how far do you cast the net and should you do it yourself or consider employing a specialist investigation company.

Whatever the case, keep records because these will be useful for law enforcement or any civil action.

Review and Monitor

If the matter is not the subject of a criminal investigation, how will you deal with the member of staff or incident in question to prevent it from happening again? What will you tell other members of staff? Review your policies, systems and processes and make any changes that are necessary to prevent a repeat occurrence. Consider testing any new procedures to ensure they are effective.

Learn

Learn from your experiences and those of others. If you have fallen victim to fraud in the past, think about how this happened and what you could have put in place to stop it. Consider training staff regularly in detecting fraud within business.

Risk Manage

This should be a continual process and form part of your overall fraud strategy. Take a risk based approach, i.e. assess the risks – the likelihood of something happening and the impact it could have on your business. If resources are limited then take action to mitigate the threats that have the most risk. To protect your business and livelihood it is vital that you manage these threats carefully.

PRACTICAL ADVICE

What follows are some simple steps which you may want to consider, when looking at preventing fraud. It is important to remember that fraud prevention is not a simple 'tick box' exercise.

It is also important that each business considers its own risks and what steps are appropriate to take in the circumstances.

Business risk

Whilst social networking is a great way of communicating, sensitive information divulged innocently or otherwise on networking sites could be damaging to your business and its image. Consider this when implementing your policies.

Intellectual property

Your Intellectual property is one of the most valuable assets of your business. Failing to protect it can put your business at risk. It is important that you understand what a patent, design, trade mark, copyright and design is and recognise your rights as a business.

Patent

If you establish a process or invent a product that could be used in an industry (i.e. it can be made) then you can apply for a patent. A patent will protect your invention by making it illegal for anyone, apart from you and someone with your permission, to produce, use, import, or sell it.

Trade mark

A trade mark is an emblem which can identify your goods or services from other businesses. This can be a sign, logo, picture, wording or a combination of all of these. You can use trade marks to help customers distinguish between your products and services from those of other businesses. They cannot be offensive or breach the law.

Copyright

This is a right that you have when creating an item such as a website, database, logo or product. It does not protect the product draft, name or purpose.

Design

A design protects the visual appearance of a product. To qualify as a new design, the overall impression of the design must be different from any other existing design.

Typically the creator of the design owns any rights in it, except where the work was commissioned or created during the course of employment, in which case the rights belong to the employer or party that commissioned the work.

There are cost implications to protecting your intellectual property but you should treat it as you would your office, your computer and your laptop. Regularly check that someone has not breached the law by profiting from your business assets and in turn, make sure you are not breaching others. Most importantly ensure you have the right level of protection, especially if you are conducting business outside of the UK.

If in doubt, always seek independent/legal advice.

For more information visit www.ipo.gov.uk

Reviewing fraud risks

When reviewing your fraud risks consider;

Location The physical location of your business. A rural business will have different risks to a high street retailer or an online business.

Business Structure Whether your business is a company, a group of companies, uses agents or partners, has one single supplier or a large number; a determined fraudster may look at how your business is structured and take advantage of that.

Markets, products and services Certain industries are more prone to fraud than others but don't let this give you a false sense of security. Maintain an awareness of current fraud trends.

Customers The nature of your customers will impact on your business risks. For example the risks from international customers who buy on credit are distinctly different from local customers paying by cash.

Suppliers and agents Do you have a small number of regular suppliers or are they wide ranging one offs?

Once you have reviewed your business and identified where you feel the biggest risks are, it is important you take action to reduce those risks; by implementing controls and procedures or passing on the risk by insuring against any loss or outsourcing a particular area or accepting the risk and any losses which may arise.

BIG SCAMS

TAKING ACTION TO REDUCE FRAUD RISK

Take action to reduce the risk on behalf of your business. Consider the following areas and suggestions. Note; this is not an exhaustive list but it does reflect the experience of the authors.

1 Conduct appropriate due diligence

It is vital for all businesses to be certain about:

- ⚠ Who their investors are
- ⚠ Who they are employing
- ⚠ Who they are doing business with

If you don't, then the chances of potentially becoming a victim of fraud are higher and may result in monetary losses with little chance of recovery.

At the same time a balance needs to be struck. You will want to be open and welcome to business; a fortress mentality may put legitimate customers off and be unnecessarily expensive.

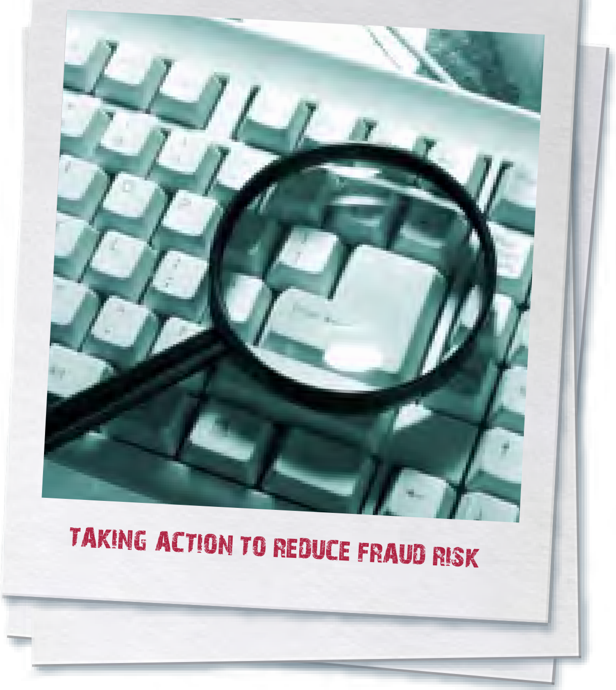
Often simple, consistently applied procedures (detailed below) will go a significant way in protecting you. Conducting due diligence checks need not be time consuming. Use the resources open to you.

2 Know your investors

Venture capital investment (money provided to startup firms and small businesses with perceived long-term growth potential) is an important source of funding for startups that do not have ready access to capital markets. It entails high risks for the investor but has the potential for above-average returns.

A company looking to invest in you will inevitably want to examine your policies and procedures. This can be a testing time as your business processes will be scrutinised for potential threats and weaknesses.

However, have you ever thought of doing the same assessment of your potential investor? They could become a long term partner and vital to the success of your business. Knowledge of their previous work, dealings with others and industry dexterity should inform your overall assessment and subsequent decision-making.



Consider the following checks;

- Visit the company web site and understand their business model (e.g. their expertise, business experiences and previous investments).
- Visit their offices and speak to people in person to assess their knowledge of your area of business.
- Consider online checks to identify other businesses that have had a relationship with the investor and contact them to see what their experience was.

3 Know your staff

Employee fraud poses a serious risk to all businesses. If your business is small, evidence shows that employee fraud has a greater impact on the success of the business. This particular fraud type is significantly under reported. You may not want to report for fear of reputational damage to the company. You may have to consider the factors around the employee and the business. You may not be able to accept the fact that a trusted member of staff could betray you. You might be concerned as to how the police will deal with the report or repercussions for the employee if they are prosecuted. Whatever your course of action is, think of this; will they go on to commit the same again?

Be aware of possible employee theft indicators

- New member of staff resigning shortly after joining.
- Staff with financial difficulties.
- Staff with a sudden change in lifestyle – cars/holidays etc.

- A pattern of customer complaints.
- Change in behaviour by a staff member – e.g. retracting from others.
- Performance drops.
- Suppliers/contractors insist on dealing with one individual.
- Staff on sick leave but working elsewhere.
- Abuses of flexible working time systems.
- Computer misuse.
- False references or false qualifications used to secure employment.

4 New members of staff

Once you have selected a prospective employee, a robust ID verification procedure is advised. Check their identity documents, take copies and retain them. Confirm their identity and their eligibility to live and work within the UK. Identity theft is a rapidly growing area of fraud and a key crime enabler.

- Obtain a variety of references to confirm the candidate's identity and background.
- Check references thoroughly and follow up with a call to all those providing references. Consider online checks; particularly relevant for key roles in your business.
- Ensure that any searches are structured and the results are appropriately recorded.
- Check **originals** of passports and driving licences etc. Ensure you retain copies on file.
- Consider training a trusted member of staff to effectively check ID documentation so they can recognise a fraudulent document. At the very least staff who check documentation should be aware of the advice available online. E.g. http://www.consilium.europa.eu/prado/en/homeIndex.html
- You may have legal requirements to abide by so check to see what is required.

- Ensure staff engaged in the selection process also consider document checks on temporary staff. Alternatively, ensure any contract with a recruitment agency stipulates that the agency will conduct all relevant checks and will be liable as a result.
- Consider asking new members of staff to sign the fact they have read, understood and agreed to adhere to any relevant policies. This will help to negate any potential argument of ignorance of procedures if instances of fraud come to light in the future.

5 Know your customer

Just as employees are important to the running of your business so too are your customers! While they are your source of revenue, customers can also pose a significant fraud risk. Here are some indicators that something may not be right;

- Unusual high value orders especially from well known companies. There has been a recent spate of fraudsters purporting to be employees of well known companies placing large orders with smaller companies. These orders have been fulfilled but have only been identified as fraud when the well known company is subsequently invoiced.

- A relatively new customer placing larger and larger orders.
- Customers requesting changes of delivery addresses at the last minute.
- Large and outstanding customer debts.
- Frequent transactions between customer accounts.

Where possible, keep the different functions of your business separate, using different staff to;

- Receive and process orders.
- Prepare and dispatch goods.
- Carry out invoicing.
- Receive payments.
- Conduct banking.

Remember that if a customer is registered with Companies House, has a VAT number and an impressive website, it does not guarantee that the customer is always legitimate. You should check as many sources as practical and appropriate to make an informed decision.

You should also be aware of the associated risks with different payment methods used by customers.

6 Checking cards – when the customer is present

When customers are paying by card, whether by debit or credit card, ensure you check the following:

- That the printed digits above or below the first four embossed card numbers are the same. This security measure features on MasterCard and Visa cards. On counterfeit cards, these four digits are often missing or rub off if you run your finger over the digits. On payment cards that have been counterfeited, they often appear but the numbers might not match.
- Always check that the title on the card matches the gender of the person presenting it.

TAKING ACTION TO REDUCE FRAUD RISK

- Be careful when customers buy goods of low value and then ask for high amounts of cash back.
- Check cards under ultra violet (UV) light which will show any anomalies. Most genuine cards have special inbuilt marks on them which only show up under UV light. If these security features are not visible and correct under UV light, then the card is counterfeit.
- You can also check receipts to make sure the number on the card tallies with the number on the receipt. Criminals copy customer card details with a small electronic gadget called a 'skimmer' and then sell these on or use the details to make counterfeit cards. The cardholder does not usually know they are a victim of fraud until they receive their statement. If you are accepting a non CHIP and PIN card payment, hold the card whilst the person is signing. This is so a fraudster cannot easily copy the signature.
- Be wary of customers who originally paid by card who ask for cash refunds or refunds to a different card.

If you are suspicious of any of the above and you believe your customer checks have failed, you should call the issuing bank.

7 Checking cards – When the customer is not present

Consumers from around the world buy products and services from UK retailers with payment cards using the telephone or the internet. Authenticating this type of payment is more challenging for both the banks and you as the business.

Ensure you are using a customer authentication service such as Mastercard SecureCode or Verified by Visa.

For more information and advice on customer present and not present, please visit:

http://www.financialfraudaction.org.uk/retail-advice.asp

or

https://www.getsafeonline.org/businesses/taking-making-payments

8 Know your suppliers

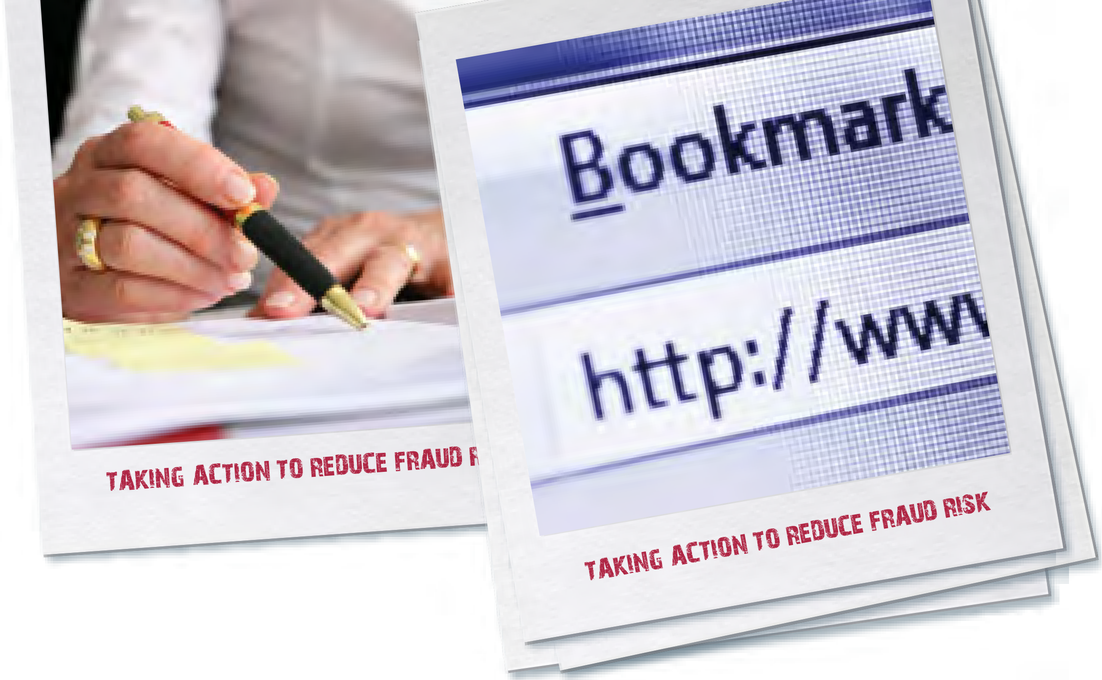
Suppliers are essential to providing SMEs with what they need to conduct business, however, they also pose their own set of fraud risks, arising internally from staff – or externally. Staff could pose as legitimate or false suppliers, or divert funds for their own use that was intended for a supplier.

Suppliers could defraud your business by overcharging, mischarging, intentionally providing poor quality or substandard goods or obtaining payment in advance for goods and services they never deliver. Suppliers may collude with others in order to artificially inflate prices or staff and suppliers might collude with each other to ensure contracts are unfairly awarded in an exchange for a 'kickback' to the employee.

Third party fraudsters could pose as existing suppliers and request changes to their payment and address details.

It is therefore vital that you understand every payment from your business and who it is going to.

- ⚠ Consider how your business identifies and selects new suppliers.
- ⚠ Consider recording the decision-making process and record and retain details of the checks on suppliers that you make along with the results.
- ⚠ Consider having a minimum level of checks to confirm the legitimacy and identity of new suppliers and changes to existing suppliers.
- ⚠ Again a risk-based approach should ensure that more robust checks are conducted on new high value suppliers.



- It is vital to check and confirm any change in supplier's bank details. Do not rely on emails or faxed messages. Check with head offices or personally with suppliers wherever possible.
- Check VAT numbers of all suppliers.
- Monitor expected spend with suppliers against actual spend.
- Rationalise and weed out unnecessary suppliers at regular intervals, e.g. every 6 months.
- Any audit should cross match all employees' bank and address details with suppliers.
- Consider background checks on suppliers, e.g. online checks and checks with Companies House. www.companieshouse.gov.uk For example, you can type into the search bar the company name to check how long they have been registered / trading. You can also see if they have submitted any company accounts. VAT numbers of all suppliers should be checked by confirming the algorithm.

9 Other good business practices

The following are some general steps that may be appropriate for your business.

- Ensure a secure and robust document destruction policy.
- Advise your staff on what to do if they suspect a fraud – e.g. have a whistle blowing policy.
- Consider a clear desk policy.
- Ensure there is an appropriate and effective staff exit procedure, that all equipment used by the employee is returned, that all access to your internal systems and building is blocked and that they have a clear understanding of what is acceptable behaviour after leaving your business.
- Consider audits, both planned and unplanned. This may be costly but you will need to weigh up the cost to the business if a fraud occurs.
- Audits should include staff expenses and procurement (spending by your business). Consider a risk-based approach so that levels of authority rise with the level of spend.
- Wherever possible, segregating different functions of your business will improve its resilience to fraud.

10 Cyber crime prevention

It is rare for a business not to use a computer for any of their functions. As computer usage increases, so too do the risks of business computers being compromised from either internal or external sources.

Therefore any business should have a strategy to deal with system error and protect against criminal compromise.

The following points should be considered.

- Ensure that staff conducting online banking on behalf of your company are aware of the potential pitfalls. For example, check the bank website is not a "phishing" site (i.e. a copy of a legitimate website used to obtain personal and bank information by deception) and that the website address shows "https" – which denotes a secure website – along with a picture of a padlock.

- Ensure an appropriate audit trail of system access is maintained so that you can identify who has accessed your company's computers, when and what functions they carried out. Determine and manage user privileges in order to do this.
- If your business is internet based consider the extent to which the personal details of staff members are shown on your website.
- Consider whether you need to comply with personal data protection legislation. If you hold personal customer information you will need to comply with customer data protection otherwise you may be liable.
- Consider employing or consulting a computer expert/IT security consultant for advice on how best to protect your business systems such as using firewalls. Ensure you have the capability to identify any unauthorised or malicious activity.
- Do you know what to do if there is a malfunction or an incidence of hacking?
- Consider routinely backing up files so that in the event of a problem, your business can continue and permanent data loss is less likely.
- Install and regularly update anti-virus software on all systems including web browsers.

- Consider using a dedicated PC for your payment transactions, reducing the risk of exposure to malware.
- Maintain an inventory of all IT equipment and software. Routinely audit the inventory.
- Manage any change in user access. Ensure that staff exiting your business no longer have access to your IT systems and building.
- Remove any software or IT equipment that you no longer need, ensuring that no sensitive information is stored on it when disposed of.
- Be extra cautious when being asked by customers and/or suppliers to change details on your payment systems. See page 37 for advice on mandate fraud.
- Some banks offer their customers free antivirus and security software. It is highly recommended you use them if available.
- Removable devices, such as USB memory sticks can be used to place malware into your data systems and for personal or business data to be extracted. Be cautious when accepting their use.
- If you are an internet-based company consider protecting your business name by registering domain names similar to your own.

11 Talking fraud – develop an anti-fraud culture

Spreading the message about your approach to fraud prevention to your employees, customers and suppliers helps to raise awareness, encourages your honest business partners to speak out when they identify fraud and promotes the message that fraud will not be tolerated.

Holding fraud awareness training sessions for your staff is one way to ensure they have recognised the issues, as is developing and implementing a simple, concise anti-fraud policy.

It is important that the messages are consistent and delivered by an appropriately senior person within the business to allow an effective anti-fraud culture to develop.

12 If fraud happens

When a business discovers that it has been a victim of fraud, not only does it come as a shock to the business and those in it, it is also an incredibly disruptive experience.

It is therefore critical to plan ahead to ensure that your business is able to function as normally as possible and that the fraud and its effects are investigated appropriately, understood and any necessary changes to business practices are identified and implemented.

Having a business plan covering these aspects will provide you with peace of mind and your business with the ability to continue whilst it deals with a case of fraud.

In setting out your business plan you may wish to determine;

- Who will be responsible for leading and co-ordinating your business response?
- Who will contact the police or Action Fraud to report.
- Who will contact the insurers if appropriate?

- Which legal and professional advisors will you contact and who in your business will be responsible for making the decision to contact them.

Always consider whether you should take action straight away or monitor and investigate further. If you investigate further, how far do you cast the net and should you do it yourself or consider employing a specialist investigation company.

BIG SCAMS

USEFUL HINTS AND RELEVANT LEGISLATION

1 Company Impersonation, Companies House and the Regulatory System

In order to protect your business's identity and details (names of directors etc) so they cannot be altered without prior notification, consider signing up with Companies House for electronic filing and PROOF (Protected Online Filing). It is a free service helping companies safeguard their data and protect them against identity theft and fraudulent filings.

For more information please visit: www.companieshouse.gov.uk

2 Holding personal information and information sharing

The Information Commissioner's Office (ICO) is an independent official body. The Information Commissioner is appointed by the Queen. The Commissioner is responsible for administering the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000.

Its mission is to uphold information rights in the public interest. They give guidance to the public and organisations, rule on eligible complaints and take appropriate action when the law is broken.

You may have to register yourself with the ICO if you hold personal information on individuals.

If you do hold personal information, you have a number of legal obligations to protect that information under the Data Protection Act. Also under the act, individuals have a right to know what information you hold on them. If they ask for this information you have 40 calendar days to respond. This is called a Subject Access Request.

You also have obligations if you are providing information overseas.

For more information on the above, please go to the ICO website www.ico.org.uk

3 Whistleblowing

In response to the Public Interest Disclosure Act 1998 you should consider putting some form of whistleblowing procedures into your business. These procedures would not apply to businesses with very small numbers of employees but should be considered by large businesses.

You should encourage your employees to raise their concerns in confidence without fear of victimisation, subsequent discrimination or disadvantage.

The policies and procedures should aim to:

- ⚠ Encourage employees to feel confident in raising issues.
- ⚠ Provide channels for employees to raise those concerns.
- ⚠ Reassure them that they will be protected from possible victimisation or retaliation if they have raised any concerns in good faith.

ATION

USEFUL HINTS AND RELEVANT LEGISLATION

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

4 The Fraud Act 2006

The act provides legislation on the offence of fraud. Although there is a general offence of fraud, there are three ways of committing it. These are:

- ⚠ False representation
- ⚠ Failure to disclose information
- ⚠ Abuse of position

In each case, it needs to be proven that:

- ⚠ The person's actions were dishonest.
- ⚠ Their intention was to make a gain or to cause a loss to another or to expose another to the risk of a loss.
- ⚠ Note; the gain or loss does not have to be permanent.

In relation to sections 2 (false representation), 3 (failing to disclose information) and 4 (abuse of position) loss or gain only extends to money and other property. Other property includes intellectual property.

Section 6 of the act applies to the possession or control of articles for use in fraud. It states that a person is guilty of an offence if they have in their possession or under their control any article for use in a fraud. This applies to all frauds under the act and can be committed anywhere.

Section 7 applies to the making or supplying of articles for use in fraud. It states that a person is guilty of an offence if they make, adapt, supply or offer to supply any article:

- ⚠ Knowing that it is designed or adapted for use in the course of or in connection with fraud, or
- ⚠ Intending it to be used to commit or assist in the commission of fraud.

'Articles' can be anything, including any form of electronic programme or data.

5 The Bribery Act 2010

This act came into effect on 1st July 2011. It creates offences of bribing, being bribed, bribery of a foreign official and failure of a commercial organisation to prevent bribery being committed on its behalf by an individual connected to it.

Section 1 states that if a person offers, promises or gives a financial or other advantage to another person, and intends the advantage:

- To induce a person to perform improperly a relevant function or activity, or
- To reward a person for the improper performance of such a function or activity,
- Then the offence is committed.

It also states where a person offers, promises or gives a financial or other advantage to another person, and

- they know or believe that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity
- The person commits the offence.

Your business needs to assess the risk of bribery, both internally and externally. Consider adopting a strategy that your business can manage and test on a regular basis in order to reduce your risk.

For more information please visit:
www.gov.uk or
www.transparency.org.uk/our-work/bribery-act

BIG SCAMS BUSINESS FRAUDS YOU MUST BE AWARE OF

eCOMMERCE FRAUD

Fraudsters will target retailers that sell goods and services online using stolen credit card details. Online business appeals to them because there is no physical contact with the business or the legitimate cardholder. Businesses should be fully aware of the risks otherwise they are more likely to be targeted.

What you should know

- When payments are accepted over the internet and processed, your business requests authorisation from the card issuer. However, this does not confirm or authenticate the customer as being the genuine cardholder. The standard authorisation only confirms that:

  a) the card has not been reported lost or stolen,

  b) there are sufficient funds available in the account, and

  c) the card number is valid.

- If a sale is subsequently established to be fraudulent and valid authentication has not taken place, the full amount may be charged back to your business if the genuine cardholder declares they did not participate in the transaction.
- Maintaining records relating to charge-backs is important. It is useful to obtain as much information as possible and provide it to your acquirer.
- If you suspect a fraudulent transaction then you need to report it to your authorisation centre.

Businesses are responsible for protecting card holder data at the point of sale and as it flows into the payment system.

For more information visit: https://www.pcisecuritystandards.org/merchants/

Minimising your risk to fraud

- Consider using the Address Verification Service (AVS), Card Security Code (CSC), MasterCard SecureCode and Verified by Visa.
- Treat high value items and overseas transactions with extra caution. Always check where the delivery address is located. If it is overseas then consider using a third party service to provide you with the details.

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

- Be wary of any changes to details initially given such as change of delivery address. Insist that you will only deliver to the customer's permanent address.
- If a courier is used, instruct them only to deliver to the address given by you, return the item if unable to deliver and always obtain signed proof of delivery.
- Be wary of your obligations when storing customers' card payment information. This data is prone to hacking so you need to ensure you are complying with data security requirements.
- Keep records of any fraudulent activity as this can be an effective way to identify patterns and areas of potential risk. Many businesses use this process to develop in-house fraud screening protection so they can predict higher risk transactions.

BUSINESS FRAUDS YOU MUST BE AWARE OF

SCAM

SCAM

ONLINE FRAUD

We now operate in a connected world, selling across multiple channels and geographies. But as the number of channels and markets we operate in continue to rise, so does the risk of fraud. Cybercriminals are becoming more sophisticated; fraud is increasingly difficult to detect and as a result standard fraud verification tools can prove to be insufficient.

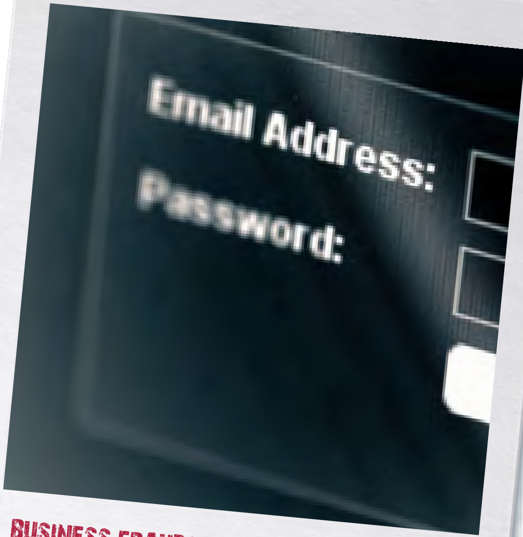
What you should know

- Fraudsters may target your online business to gain customer information such as names, addresses and payment details to commit crime.
- 26 million people in the UK use public Wi-Fi networks e.g. when travelling on business at hotels, bars, cafes etc and 42% take no steps to secure their connection when sending personal and business emails, banking or credit card details. These networks are open to hacking, identity theft and fraud. Numerous simple tools and free apps exist which can be used to hack public Wi-Fi networks – a process called 'sniffing'.
- Employees are now being targeted by what's known as 'spear phishing' – when an email is sent by a fraudster directed at a particular individual. They pose as someone else within the company, usually someone important or in a position of trust. They request information such as login IDs and passwords. They may ask the employee to update their username and passwords. Once the fraudster has this information, they can access the secured networks of your business, gaining entry to confidential information and customer data.
- Other methods include asking the employee to click on a link, which deploys malware that can take personal or confidential data from within your business.
- Be wary of where you store your information. If you employ a third party 'hosting' company then you need to identify where your information is being kept, how it is being shared and how is it being stored.
- The latest computer threat to businesses is called **Cryptolocker**; a form of

ransomware that is usually disguised within a legitimate looking email attachment. When the attachment is opened, the malware encrypts certain types of files within your computer. You will then receive a message offering to decrypt the data in exchange for payment usually via Bitcoin or pre-paid vouchers. There is little recourse for the victim and that is why it is important to back up your data on a regular basis.

Minimising your risk to fraud

- It is essential that you back-up data otherwise the impact this may have on your business can be huge.
- Ensure your passwords are robust by using a mixture of upper and lower case letters, numbers and symbols. Do not use obvious passwords, like your mother's maiden name as this is information that can be easily obtained by a fraudster.
- Always challenge giving out your personal or financial details to anyone.
- Whatever security systems you have in place, test them to see that they are working appropriately and are not vulnerable to invasion. This includes your website.
- If your bank offers it, consider using dual authentication. This can reduce your fraud risk from malware and insider threats.



BUSINESS FRAUDS YOU MUST BE AWARE OF

LONG AND SHORT FIRM FRAUD

This is when criminals hijack or set up an apparently legitimate business with the intention of defrauding both its suppliers and customers. They are happy to deal in any goods or services that have a market value, preferably those that are not traceable and easily disposable – e.g. electrical goods, toys, wine and spirits, confectionery etc.

What you should know

Long firm fraud; Your business has developed a beneficial relationship with a company that has a good reputation and credit history. The company places lots of small orders with you, paying promptly. You trust this company as a supplier. The company however, changes its activity and starts making much larger orders with your business. You supply your goods but the company disappears without paying you and sells the goods on.

Short firm fraud; Your business supplies to another business which has only operated for a short time. If it is a limited company, it will often have filed several sets of false accounts and director appointments at Companies House within a short space of time. It may also provide false trade references to make itself appear credit worthy. The company will have no day-to-day trading activity. They will use credit to obtain goods from your business that are delivered to third-party addresses. Again the company will disappear without paying you and will sell the goods on for cash.

Minimising your risk to fraud

- ⚠ Obtain full details of customers including personal details of those in control.
- ⚠ Obtain trade references. This needs to be from more than one source and follow up with the companies as to how long they have known the business for.
- ⚠ Ensure you complete address checks to confirm their business address and ideally contact the directors of the company to ensure you are happy with who they say they are.
- ⚠ Complete checks with Companies House along with banking references and well known credit reference agencies,

to identify any unusual filing patterns or dramatic increase in credit searches. If this is too expensive use open source checks. Searching on company directors, addresses and trade names can be vital information for you.

- ⚠ If you have time, consider visiting potential new customers for proper on site inspection.
- ⚠ Obtain landline contact numbers (not just mobile). Confirm these details and check they answer the phone in the correct company name.
- ⚠ Do not accept handwritten orders or faxes.

MANDATE FRAUD

Mandate fraud occurs where someone tricks you into altering details of a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example a business supplier, a subscription etc. It is a simple but all too often effective fraud and is therefore commonly used. Huge amounts of money can be easily stolen.

What you should know

- Your business may be contacted by someone pretending to be one of your suppliers. They inform you of a change of bank details and that you need to amend their account to reflect this. You therefore amend the details. However, the following month you are contacted by the genuine supplier asking what has happened with your monthly payment. You realise you have been a victim of fraud.
- Your business may be contacted by someone pretending to be from an organisation you have a standing order with. They request you change an order to reflect a change in their banking. The standing order mandate is changed accordingly but the following month the actual organisation fails to deliver your products or a membership has been cancelled as they did not receive their payment.
- Your business may receive a letter in the post that appears to be from the company supplying a monthly magazine to you. It provides details of a new bank account and asks you to change the payment details to reflect this. The direct debit mandate is amended as instructed. The following month your magazine does not arrive. You contact the publisher and are told that because your payment was cancelled you no longer have a subscription for the magazine.
- You may discover your business online bank account has been hacked into and monthly payment details are altered so that money is transferred into a fraudster's account.

Minimising your risk to fraud

- Do not simply rely on faxed information, emails or mobile telephone calls. Take action to verify and corroborate any request to change suppliers' bank details.
- Always verify changes to financial arrangements with the organisation directly, using established contacts you have on file wherever possible.
- Maintain records of standing orders and direct debits.
- Keep bills and other business documents in a secure place to prevent information falling into the wrong hands.
- Check your bank statements carefully for anything suspicious.
- Notify your bank immediately if you see any unusual activity on your account.

COMPANY IMPERSONATIONS

Also known as 'corporate identity theft'

Should you receive a call from a person claiming to be from a company that you have a business relationship with and you are suspicious about the nature of the call or the caller's identity, then consider the following advice:

- Ask a number of questions that only you and the genuine company know the answer to, e.g. a contract number or purchase order number.
- Ask for any request to be emailed.
- Call the genuine company using your regular contact number and employee you deal with at least five minutes after ending the initial call as the phone line may have been kept open by the fraudster. Alternatively, simply use another telephone line.

CHEQUE FRAUD

Genuine cheques can be stolen, altered and presented – or counterfeited and presented.

What you should know

- Where possible, only accept cheques from people you know and trust.
- Do not release goods until you are sure that the funds are yours.
- Use the checker at www.chequeandcredit.co.uk to check clearing timescales.
- Do not accept cheques made out to a higher value than you are expecting.
- Be particularly cautious with new customers who place large orders, make overpayments and then request refunds, or request immediate delivery or change their delivery address after the order has been placed.
- This method is often used in employment opportunity scams or transactions for goods and services sold through classified adverts.

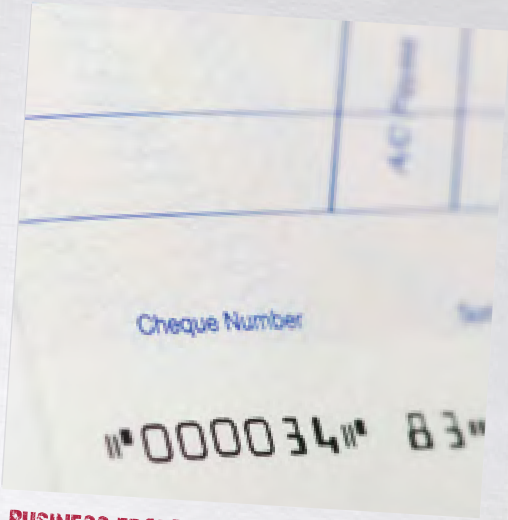
Minimising your risk to fraud

- Always use indelible ink based pens or black or blue ballpoints pens. If you enter details with a printer, make sure approved machines and toners are used. This makes it harder to alter or erase the writing. A list of approved machines is available at www.chequeandcredit.co.uk
- Ensure any blank spaces on cheques are crossed through with a pen. For example, after the payee name and after the payment amount written in words. If you enter details with a machine, ensure that software adds in any blank spaces with asterisk (*) symbols.
- Do not leave large spaces between words. If you use a machine, ensure the software uses "zero" instead of "nil". This can easily be fraudulently changed to "nine."
- If you are due to receive a new cheque book and it doesn't arrive, contact your bank. Consider collecting business cheques from the bank as they are vulnerable to theft from the postal system.

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

- ⚠ Regularly check your bank statements to keep track of cheque payments.
- ⚠ Avoid using a sole signatory within your business. This allows any discrepancies to be picked up by others.

SCAM



BUSINESS FRAUDS YOU MUST BE AWARE OF

BUSINESS FRAUDS YOU MUST BE AWARE OF

PROCUREMENT FRAUD

Procurement fraud is on the increase. Your employees may be trusted with certain procurement responsibilities which can provide opportunities to commit fraud. Identifying the risks is difficult. However a common sense approach is always essential.

What you should know

- It is often possible for an employee to create a record for a fictitious company or a legitimate company that does not provide services to your business. This provides an opportunity to transfer money to the recipient, controlled by either the employee or an outsider.
- Customer fake invoice scams occur when fraudsters send an invoice or bill to a company, requesting immediate payment for goods or services. The invoice might say that the due date for payment has passed and threaten that non – payment will affect credit rating. In fact the invoice is fake and is for goods and services that haven't been ordered or received.
- An employee could intercept and alter payee details and amounts on cheques and Payable Orders, then attempt to cash them.
- Suppliers may try to encourage business by offering anything of value to influence a business decision.
- Your employee may self-authorise payments for themselves or there may be collusion with employees and suppliers to gain contracts.
- There may be conflicts of interest. An employee may have a financial interest in the success of a particular supplier but their goods and services may be at a higher rate which may be detrimental to your business.

Minimising your risk to fraud

- Never change payment details on the basis of a telephone call or email. If you do receive such a call, verify with an existing contact that this is correct before processing any new changes.
- Ensure that there is a need for the goods or service being provided.
- Review your accounts on a regular basis to identify any anomalies in your payment processes.
- Empower staff to identify and challenge inappropriate behaviour.

TELEPHONE FRAUDS

If fraudsters hack into your business phone lines they can gain personal or confidential information which could potentially be damaging to you. Make sure you have the necessary security systems in place to protect you.

What you should know

Telephone/video conference hacking

You may routinely interact with other businesses through confidential conference telephone or video calls. It is an effective way to communicate and minimises disruption to your day-to-day working through wasted time, resources and expense. However, these calls can also be accessed by fraudsters who obtain passwords and codes through overhearing conversations and unprotected emails.

PABX hacking

'Private automated branch exchange' telephone networks are commonly used by call centres and other businesses and organisations. It is a single access number that has multiple lines to outside callers and also provides a range of external lines to external callers or staff. Fraudsters will use vulnerabilities to hack your system, access passwords and listen into conversations and voicemails. They can also use your PABX system to make international or long distance calls often to premium rate numbers that the fraudster has set up. Your business will unknowingly let the fraudster sell on the access and use of your system, increasing your phone bills by thousands of pounds. It will be your business who is responsible for any fraudulent usage of your system; not the telephone provider.

These frauds often occur over the weekend or bank holiday periods where staff are out of the office for long periods, providing fraudsters with an opportunity to rack up huge bills on behalf of your company.

Advice to SMEs on how to take steps to avoid Vishing

Vishing occurs when criminals use the telephone to call you, pretend to be from a legitimate business and persuade you to surrender private information that they can then use for financial gain. It's the telephone equivalent of phishing.

Be wary of

- ⚠ unsolicited approaches by phone.
- ⚠ cold callers who suggest you hang up the phone and call them back. Fraudsters can keep your phone line open by not putting down the receiver at their end.

Never disclose your company's

- ⚠ 4 digit card PIN to anyone, including the bank, police or another organisation.
- ⚠ passwords or online banking codes*.
- ⚠ financial details – unless you are sure who you are talking to.

Your bank, the police or another organisation will never

- ⚠ ask for your organisation's 4 digit card PIN.
- ⚠ ask you to withdraw money to hand over to them or transfer money to another account, even if they say it is in your organisation's name.
- ⚠ come to your organisation to collect your business account card or cheque book.

Remember

- ⚠ Use a different phone line to return a call if you have access to one.

- ⚠ If you are unsure about providing the information a caller has requested, check your organisation's policy on what information you should and shouldn't provide to a caller.
- ⚠ If you are suspicious or feel vulnerable, don't be afraid to terminate the call, and say no to any requests for information.
- ⚠ Criminals may already have basic information about your organisation in their possession (e.g. name, address, account details). Do not assume a caller is genuine even if they have details or knowledge about you and your organisation.

* Different banks use different systems or authentication devices to prove that you are the genuine customer/business. Some may issue you with a key-fob device that produces a one-time passcode. Others may provide you with a pocket-sized card reading device that you insert your debit card into, which also produces a one-time passcode. This passcode can then be used as one of the security steps needed to login to your organisation's online banking website or to authorise a payment.

Minimising your risk to fraud

- ⚠ Educate yourself on the systems within your business to enable you to detect any suspicious activity.
- ⚠ Ensure that your systems are kept in a secure location. You may need to consider locked areas if you use office space with multiple occupancy.
- ⚠ Always use strong passwords, manage access to them and never use default password settings.
- ⚠ Consider using settings that restrict international or long distance calls. You can also contact your telephone provider to request this restriction.
- ⚠ If you are using video conferencing through internet based calls such as Skype, ensure you are using up to date anti-virus and firewalls. This will also help protect you from PABX hacking.
- ⚠ Familiarise yourself with your business call patterns and consider monitoring them, especially if there are calls out of hours, weekends and bank holidays.
- ⚠ Always keep your software up to date, especially if you are using PABX.

COMPANY HIJACK

Company hijacks normally involve fraudsters changing the details of company directors and registered offices. To combat this consider joining the Companies House PROOF scheme and register with the webfiling service.

Company hijack can often precede short firm fraud activity.

INSOLVENCY-RELATED FRAUD

Fraud relating to bankruptcy and insolvency can involve companies fraudulently trading immediately before being declared insolvent – or phoenix companies.

Phoenix companies are companies set up immediately following the insolvency of another with the same directors, but are not liable to pay for the losses of the previous company because they are different entities. Phoenixism can be perfectly legal. Fraud happens when directors abuse the phoenix company arrangement by transferring the assets of the failing company below their market value before insolvency. By doing this, the fraudulent directors reduce the funds available to creditors when the original company becomes insolvent. As a result, the creditors are left out of pocket for the goods or services they supplied. Other associated offences include the reuse of prohibited names or directors acting whilst disqualified.

BUSINESS FRAUDS YOU MUST BE AWARE OF

BUSINESS DIRECTORY FRAUD

Your business may receive a form in the post, by email or fax, appearing to offer free listings in a business directory. You will be asked to return the order form even if you decline to place an order. However, in the small print it states that by returning the form, you are committing to an order and will pay for ongoing entries in the directory. This will then cost your business hundreds of pounds a year.

An increasingly common scam occurs where businesses are contacted by telephone offering advertising space in a publication which is allegedly linked with the emergency services, linked to a recognised trade body or purports to be an industry specific magazine.

In some cases companies are sent a glossy copy of the magazine to encourage the placing of an advert. However, often these magazines are not actually printed in bulk or distributed and if they are, the circulation list is not at the level described. In some instances businesses have received debt recovery letters for adverts they did not agree to place.

Ensure you do your research before agreeing to anything.

OFFICE SUPPLY FRAUD

This fraud type occurs where telemarketers trick employees into ordering and paying for stationery, e.g. toner cartridges.

The caller may mislead a company's employee into thinking an order for office supplies has already been placed, either by an existing or former colleague. To further convince them it is genuine, the caller states they are chasing up a signature to complete the order.

The company is then invoiced for unwanted, and often overpriced, stationery and office supplies.

If the company tries to return the goods, they are told that returns are not possible because the order form has been signed and the order was agreed over the phone.

If a member of your staff has a responsibility to purchase office equipment, consider due diligence. Always refer back to your existing contacts within the business and if they are not regularly known to you conduct further checks. A risk based approach will help prevent fraud.

FRAUD DOES HAPPEN

PABX HACKING FRAUD

A small UK business ended up paying over £50,000 in call charges as a result of their office telephone system being hacked.

The staff closed business one Friday afternoon for a long bank holiday weekend, switching the office telephone system to “automatic attendant.”

After the long weekend, the staff opened the office, operating business as normal.

At the end of the month, the postman delivered the mail including the latest telephone bill:

£50,107.35 including VAT!

There must have been a mistake as the average quarterly bill was usually around £10,000. The office manager called the telephone company and highlighted what she believed was a major billing error.

WRONG – the bill was correct!

On further inspection it appeared that £45,356.90 of calls were made to international destinations which began over the Bank Holiday period and had continued every evening since that time.

The business telephone system had been “hacked” which allowed fraudsters to route telephone calls through their system to high rate destinations.

After negotiation with the telephone supplier the bill was reduced to £32,000. This was still twice what the office would normally pay.

Do you know if your office telephone system is secure?

SCAM

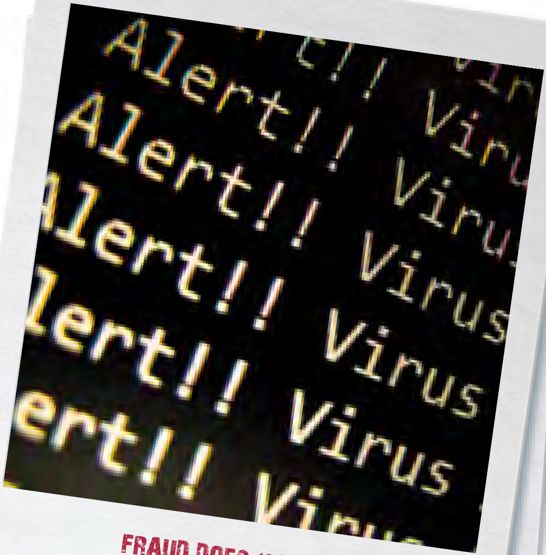
CRYPTOLOCKER FRAUD – RANSOMWARE

A member of staff in an SME opened an email and clicked on a link that in fact contained malware. The malware infected the computer system and encrypted all files so that no access could be gained by members of staff.

The criminals contacted the company giving 24 hours to pay £300 in Bitcoins to unlock their system. The company was particularly vulnerable as they had not backed up their files.

They had not heard of Bitcoin or how to source them and had to employ a computer consultant at short notice to enable them to make the payment. Once the Bitcoins were obtained, payment was sent to the criminals who then provided access to the system.

There is no guarantee that your computer system will be unlocked if you pay. Consider seeking professional help.



FRAUD DOES HAPPEN

BIG SCAMS

HOW TO REPORT

Reporting crime, including fraud, is important. If you do not tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim, however minor, there may be other businesses in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

Where to report

Report to Action Fraud online at www.actionfraud.police.uk

Or telephone; 0300 123 2040.

Unless:

- ⚠ A crime is in progress or about to be.
- ⚠ The suspect is known or can be easily identified.
- ⚠ The crime involves a vulnerable victim.

If this is the case you should contact police directly either by dialling 999 in an emergency, or dial 101 or go into your local police station.

The Business Crime Hub (BCH) is a central unit created in 2013 to encourage a consistent approach to tackling business crime throughout the MPS.

Through liaison with the business community, Mayor's Office for Policing and Crime (MOPAC) and local Police, the BCH works to improve crime prevention and reduce crime affecting businesses throughout London. The BCH also provides specific help and advice to communities that would like to form a Business Crime Reduction Partnership (BCRP) and BCRPs that are looking to improve their own services.

The Business Crime Hub has the following aims:

- To coordinate delivery of the MOPAC Business Crime Strategy;
- To advise and share best practice with Business Crime policing contacts in every Metropolitan Police Service (MPS Borough;

- To promote creation of Business Crime Reduction Partnerships (BCRPs). These include intelligence and information-sharing between business and police, shared radio link systems, CCTV, working alongside private security and managing exclusion notice schemes
- To encourage partnership between businesses , private security and Police;
- To set standards for BCRPs and Information Sharing Agreements (ISA);
- To act as the MPS single point of contact for business crime.

Included in the hub are the work of the Designing Out Crime Officers (DOCO's) They provide guidance on the designs of the built environment, minimising the opportunity for crime to occur.

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

FURTHER ADVICE

Below is a list of websites that you may find useful:

www.met.police.uk/fraudalert

www.actionfraud.police.uk

www.financialfraudaction.org.uk

www.fraudadvisorypanel.org.uk

www.fsb.co.uk

www.cifas.org.uk

www.bis.gov.uk/insolvency

www.bis.gov.uk

www.getsafeonline.org

www.companies-house.gov.uk

www.fraudadvisorypanel.org

www.fca.org.uk

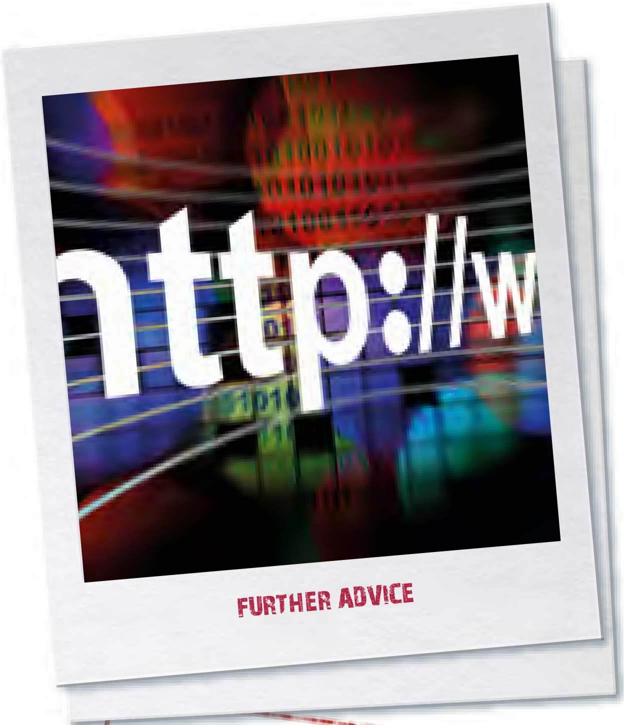
www.hmrc.gov.uk

www.ipo.gov.uk

www.ico.org.uk

www.pcisecuritystandards.org

www.chequeandcredit.co.uk



FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

USEFUL CONTACTS

BIS

The Department for Business, Innovation & Skills (BIS) is the department for economic growth. The department invests in skills and education to promote trade, boost innovation and help people to start and grow a business. BIS also protects consumers and reduces the impact of regulation.

BIS is a ministerial department, supported by 49 agencies and public bodies.

Tel: 020 7215 5000
Web: www.bis.gov.uk
Address: 1 Victoria Street
London SW1H 0ET

Companies House

The United Kingdom has enjoyed a system of company registration since 1844. Today, company registration matters are dealt with in law, by the Companies Act 2006.

All limited companies in England, Wales, Northern Ireland and Scotland are registered at Companies House, an Executive Agency of the Department for Business, Innovation and Skills (BIS). There are more than 3 million limited companies registered in the UK, and more than 400,000 new companies are incorporated each year.

The main functions of Companies House are to:

- incorporate and dissolve limited companies;
- examine and store company information delivered under the Companies Act and related legislation; and
- make this information available to the public.

Telephone: 0303 1234 500
Email: enquiries@companies-house.gov.uk
Address: Companies House
Crown Way
Cardiff CF14 3UZ

Federation of Small Businesses (FSB)
The FSB is non-profit making and non-party political.

The Federation of Small Businesses is the UK's largest campaigning pressure group promoting and protecting the interests of the self-employed and owners of small firms. Formed in 1974, it now has 200,000 members across 33 regions and 194 branches.

Web : www.fsb.org.uk

Financial Fraud Action UK (FFA UK)
Financial Fraud Action UK works in partnership with The UK Cards Association on industry initiatives to prevent fraud on credit and debit cards.

The UK Cards Association is the leading trade association for the cards industry in the UK. With a membership that includes all major credit, debit and charge card issuers, and card acquiring banks, the role of the Association is both to unify and represent the UK card payments industry. It is responsible for formulating and implementing policy on non-competitive aspects of card payments including

codes of practice, fraud prevention, major infrastructural changes, development of standards and other matters where cross-industry benefits are identified.

Web: www.financialfraudaction.org.uk

Fraud Advisory Panel

The Fraud Advisory Panel is a registered charity and membership organisation which acts as an independent voice and leader of the counter fraud community in the United Kingdom.

It brings together people and organisations with an interest and expertise in preventing, detecting, investigating and prosecuting fraud.

Tel: 020 7920 8721 (general enquiries)
0207 920 8637 (membership and events)
Web: www.fraudadvisorypanel.org
Address: Fraud Advisory Panel
Chartered Accountants' Hall
PO Box 433
Moorgate Place
London EC2P 2BJ

Insolvency Service

The Insolvency Service is an Executive Agency of the Department of Business, Innovation and Skills (BIS). The Company Investigations team within the Insolvency Service has the power to investigate limited companies where information received suggests corporate abuse; this may include serious misconduct, fraud, scams or sharp practice in the way a company operates.

To complain about a limited company that is still trading:

Tel: 0845 601 3546
Email: intelligence.live@insolvency.gsi.gov.uk
Web: www.bis.gov.uk/insolvency
Address: Intelligence Hub
Intelligence & Enforcement Directorate
Investigation and Enforcement Services
Insolvency Service
3rd Floor Cannon House
18 Priory Queensway
Birmingham B4 6FD

HMRC
Her Majesty's Revenue and Customs

Web: www.hmrc.gov.uk

Financial Conduct Authority (FCA)
Regulates the financial services industry in the UK. Their aims are to protect consumers, ensure the financial industry remains stable and promote healthy competition between financial services providers. The FCA has rule-making, investigative and enforcement powers that are used to protect and regulate the financial services industry.

Tel: 0845 606 9966 (call rates may vary)
Email: fcc@fca.org.uk
Web: www.fca.org.uk

Information Commissioner's Office (ICO)
The UK's Independent Authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Tel: Helpline 0303 123 1113 or 01625 545745 between 9am and 5pm, Monday to Friday
Web: www.ico.org.uk
Address: Head office
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

FIGHT FRAUD
TAKE ACTION TO PROTECT YOUR BUSINESS

This booklet has been written and produced by the Metropolitan Police's Operation Sterling Team. We would like to thank the following for their contributions to this booklet:

Brendan Weekes – Smith & Williamson LLP

Financial Fraud Action UK

Insolvency Service

Published by the Metropolitan Police Service

BIG SCAMS