DON'T let information fall into the wrong hands.

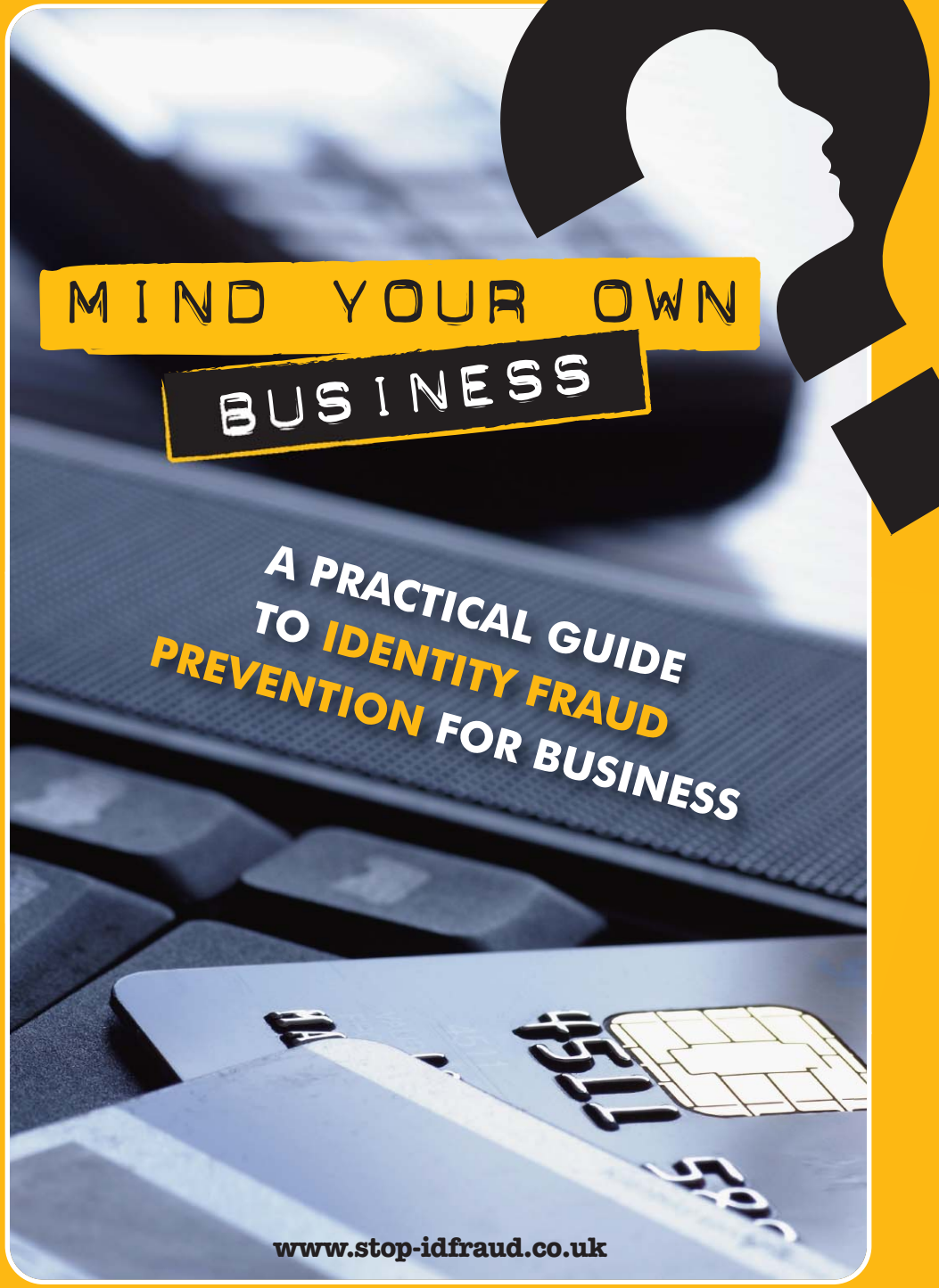
For more information on identity fraud and how to protect yourself, your business and your customers visit **www.stop-idfraud.co.uk**

NATIONAL IDENTITY FRAUD PREVENTION WEEK™

Supported by:

Fellowes · Royal Mail · CIFAS · National Fraud Authority · British Chambers of Commerce · Metropolitan Police · FSB Federation of Small Businesses · City of London Police · British Retail Consortium · Equifax · Experian · Callcredit · Home Office Identity & Passport Service

Literature Code: 361060



FOREWORD

Mike Cherry
Home Affairs Chairman
Federation of Small Businesses

"Research by the Federation of Small Businesses (FSB) shows that 6% of businesses have been victims of corporate identity fraud in some form.* While some may think that 6% does not sound like a large number, it amounts to nearly 13,000 of our members - a figure we want to ensure does not rise. Identity theft is a huge headache for businesses and can be expensive, both in terms of direct costs and time taken to resolve the issues.

The problem is that identity theft can happen in a multitude of different ways and businesses need to be on their guard to protect their sensitive business data, and that of their staff and customers. Corporate identity fraud can happen through fraudsters changing companies' details via Companies House, the hijacking of Web domains, fraudulent mortgages and direct debits set up via banks, and even discarded papers or CDs in the rubbish. The list goes on. Businesses also need to be particularly vigilant about phishing emails. Though the danger posed by these seems to be increasingly common knowledge, they are an ever-changing threat, with more sophisticated Web site links appearing that fool those who aren't prepared.

Businesses: please read this guide and see how you fare on the checklist for preparedness. Does it reflect how your business operates? Do your bit to raise awareness of ID fraud: report fraud to your bank or police service as and when it happens to improve the picture of fraud in the UK. The National Fraud Reporting Centre will give you an opportunity to do this, and will give you greater support and advice on how to prevent your business becoming a victim of fraud. Get involved in your local Fraud Forum and access advice and updates on current threats.

You will find a range of good advice and helpful information in this guide to help you and your business minimise the risk of identity fraud."

**Inhibiting Enterprise: Fraud and online crime against small businesses 2009*

CONTENTS

OVERVIEW..... p03
IDENTITY FRAUD AND YOUR BUSINESS..... p04
SHOULD YOU BE WORRIED?..... p07
- Data Protection Act..... p10
- PCI-DSS..... p11
- PROOF..... p12

TRENDS IN FRAUD..... p13
WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?..... p15
- Identity Verification..... p18
- Information destruction..... p19
- Online security..... p20
- Checklist..... p22

WHAT TO DO IF YOUR BUSINESS BECOMES A VICTIM..... p23
WHAT CAN YOU DO TO PROTECT YOUR OWN IDENTITY?..... p24
AFTERWORD..... p26
ABOUT THIS GUIDE..... p27
USEFUL CONTACTS AND RESOURCES..... p28

OVERVIEW

The term **'corporate identity fraud'** refers to the impersonation of an organisation for financial or commercial gain. Typically, a false company trades or steals another's identity and/or financial information to purchase goods and services, obtain private information or to access private facilities in the real organisation's name. Though the mainstream press often focuses more on personal ID fraud, its business counterpart is a real and serious threat, and the battle against it continues to evolve, with companies and associations forced to find ever more sophisticated ways to deal with ever more sophisticated criminals.

"Fraudsters may try to steal your goods, business identity or tap into your business to launder money."

Approaches may be made through letters, phone calls, emails or even by going though your rubbish. Typical scams include investment offers or opportunities to acquire new customers who you supply but from whom you never receive payment. '*Phishing*' scams are a prime example, where personal or business banking details are requested, and though many give themselves away with poor spelling and grammar, the con is becoming increasingly convincing with apparently-real Web pages and contact information.

Corporate identity fraud may be used for a variety of reasons, from simple personal financial gain right through to money laundering and even financing terrorist activities. VAT fraud, or 'Missing Trader Intra-Community fraud' (carousel) fraud alone costs the UK an estimated £3 billion every year. While such fraud is carried out by organised gangs, businesses too have a responsibility to help in reducing it or they may become liable for investigation by HMRC. Not for nothing are identity fraud and its associated activities increasingly referred to as an industry in their own right.

A report by **Fellowes for National Identity Fraud Prevention Week showed that 36% of businesses** don't have a comprehensive policy or procedure in place to help prevent identity fraud. It doesn't take much to get started – even something as simple as shredding sensitive documents before disposing of them helps the fight immeasurably, yet is often overlooked owing to lack of internal communication, education and enforcement.

The issue is compounded when businesses do not protect themselves sufficiently against identity fraud: If fraudsters are able to set up a false supplier account with one business, it gains a certain amount of credibility, which in turn makes it easier for them to defraud still other organisations. What's more, the current tough economic situation means corporate identity fraud is on the increase because criminals too are desperate for money, and companies can be tempted to relax their security checks in an effort to book in extra revenue more quickly.

This guide aims to give you the basic facts to help you in the ongoing battle against corporate identity fraud, especially where it concerns the small-to-medium sized business, which can ill afford the financial and reputational losses that result from it.

Identity fraud affecting a business comes in several different forms: Let's consider corporate identity fraud first. The two most common varieties are company hijacking and company impersonation. The former concerns a fraudster submitting false documents to Companies House to change the registered address of an organisation, often including appointing 'rogue' directors. Goods and services are then purchased on credit, sometimes through a reactivated dormant supplier account, but are never paid for, leaving the real organisation with the bill.

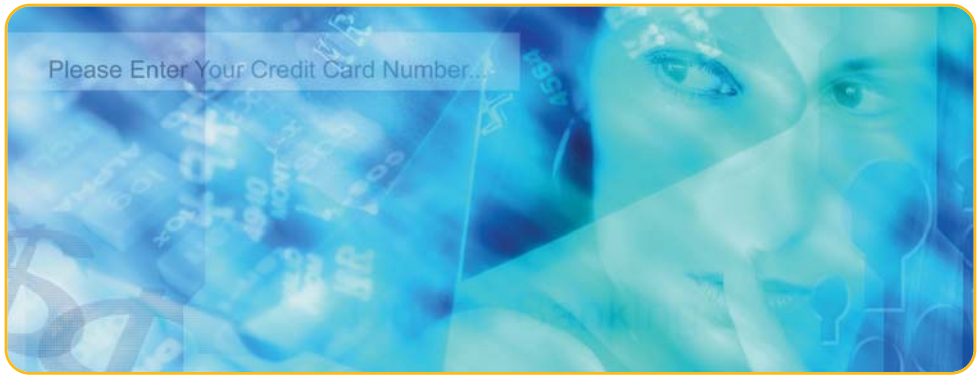
Company hijacking and impersonation

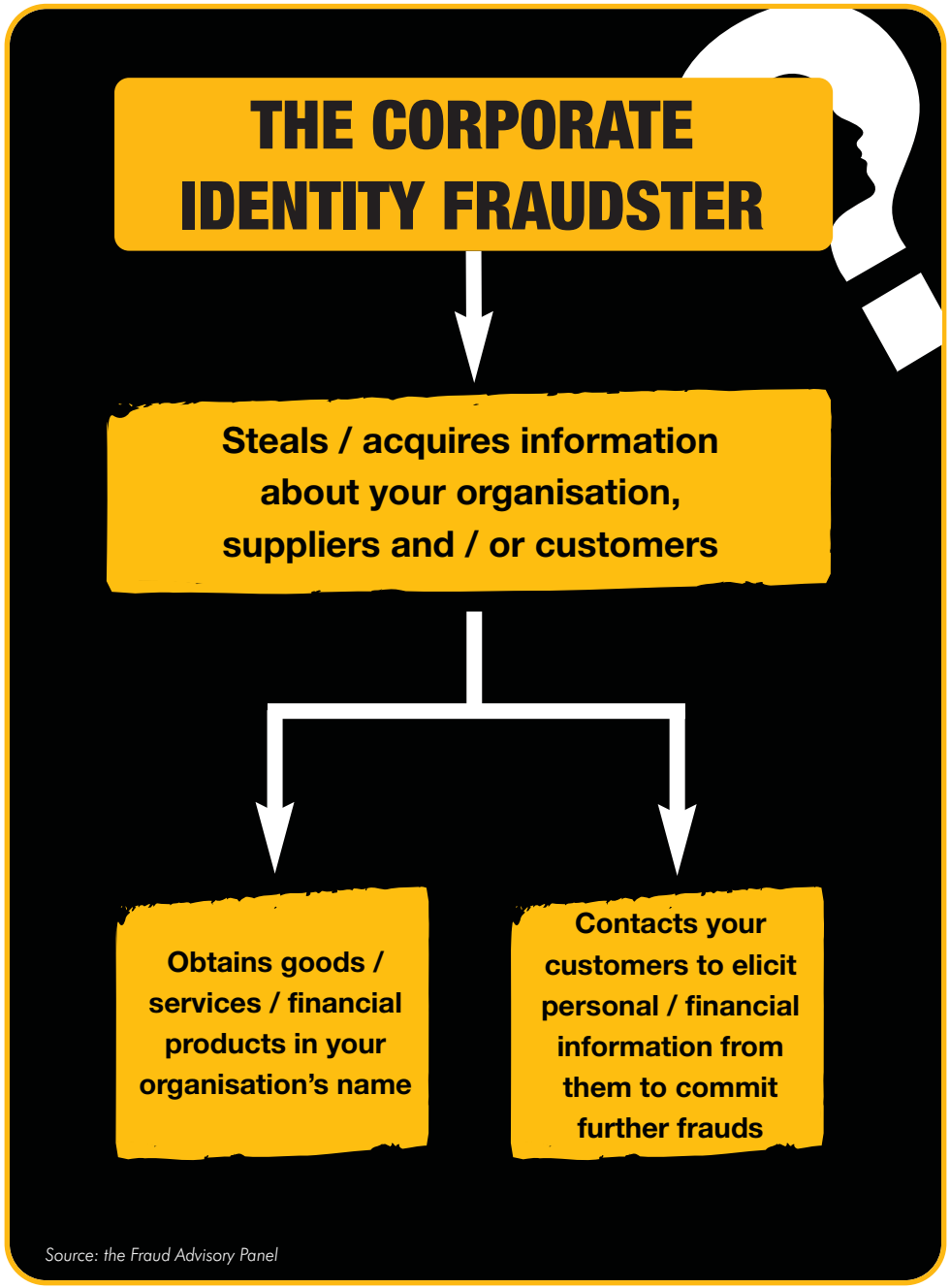
In the case of the latter, the fraudster impersonates a business to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them. Probably the most well-known example of this is a phishing email. Your personal email account and the corporate email accounts of each of your employees probably collect hundreds of these every day in spam filters, but plenty still get through and, as the con becomes more convincing, still fool tens of thousands a year. Fake Web sites and invoices are also common tools in company impersonation, and the damage done to the brand and customer relationships of real organisations by such activities is huge.

In both cases, the scam works in much the same way, with the information the fraudster seeks to acquire or steal including:

- Organisation name and company number (*if incorporated*)
- The address of the registered office
- Information relating to directors, employees and/or customers
- Details of supplier accounts, which are used to:
  - Acquire financial products (e.g. *loans and corporate credit cards*)
  - Order goods and services on credit
  - Hijack company bank accounts
  - Deceive customers
  - Purchase assets

Crooks will even sometimes change a business's details (e.g. directors or registered address) with Companies House in order to facilitate the criminal activity. Alternatively a fraudster may simply set up a false company to purchase goods and services on credit from your organisation and disappear before paying for them. Organisations can be vulnerable to corporate identity fraud committed internally by employees, externally by individuals or organised criminals, or in collusion.





IDENTITY FRAUD AND YOUR BUSINESS

Fraudulent customers or suppliers

Companies are also at risk from identity fraud in other ways, including from fraudulent customers and suppliers. Fraudulent customers are those who will 'buy' products or services and then never pay for them. A typical example would be Cardholder Not Present transactions, where the fraudster provides another person's identity and financial details to close a purchase. Only weeks or months later does the company find itself out of pocket when the real card holder reports the transaction as fraudulent. Fraudulent suppliers set up a fake company (at varying levels of sophistication) and obtain payment from a business for products or services which then never appear.

Information breaches

Finally, a business may unwittingly put its staff, customers and suppliers at risk of identity fraud by, for example, not protecting sensitive information like financial statements, employee records and contact details. Often, the rubbish bins of legitimate organisations make for rich pickings for criminals which not only perpetuates the identity fraud industry but does serious damage to the company's reputation when the source of the leak is discovered by irate customers. What's more, under the *Data Protection Act*, it is illegal to dispose of such information without thoroughly destroying it first, for example with a cross-cut shredder. Yet worryingly one third of employees are still throwing away documents without shredding them first so it isn't surprising that only 3% of consumers feel totally confident that their personal data is being handled securely by businesses. What about your customers?

Protecting a business on and off-line against identity fraud requires constant vigilance against increasingly wily criminals. Getting the right technology to protect IT systems is vital, but perhaps even more important is putting the right policies and processes in place to tackle the threat, and this guide will outline the risks and the initial steps that you can take to protect your business.

SHOULD YOU BE WORRIED?

Case study: 'Stuart'

"It happened to me"

Stuart runs his own coaching and training company for businesses. He had his wallet stolen whilst attending a training course in Northampton. As soon as he noticed, he called all his banks to put a stop on his cards, but due to the fact that he was told he did not answer all the security questions correctly, the banks were unable to take any action. On returning home, his wife informed him that someone from the council had called earlier that day, claiming they had a returned cheque from a council tax refund, and were calling to check Stuart's address. She gave the caller their address and corrected him when he got Stuart's mother's maiden name wrong. Stuart's bank had also called that day. Unable to get in contact with him, they said they would call back later, and reassured his wife that everything was fine.

What in fact had happened was that criminals had used the personal information from Stuart's credit card, driving licence and conversation with his wife to fake his identity and fraudulently take £4,000 from his business account, £300 from his personal bank account, £14,000 from his Visa card, spent £2,500 to buy a video camera and £1,000 in a clothing shop. The incident was seriously stressful for both Stuart and his wife and affected their business and personal accounts. For Stuart this was a major distraction to his coaching and training business due to the time spent trying to solve the crime. It took four months to get his identity back and deal with the repercussions of the crime. In addition, Stuart had to go away for a business trip the day after the incident, and had to borrow money to fund it.

Case study: 'Beaverbrooks'

"It happened to my company"

In 2001, Beaverbrooks launched its Web site, which has proven to be very successful. Since the launch, sales via this channel have seen 100% growth year on year and online sales now equate to the equivalent of three Beaverbrooks superstores. Selling via the Internet, however, is not without its challenges. The value of items that can be ordered from Beaverbrooks online can range from less than one hundred to many thousands of pounds. As a result of this, and also due to the fact that jewellery can be easily re-sold, the Web site became a prime target for criminals.

When the site was first launched it had no fraud prevention measures in place and it was hit by groups of organised criminals in fraud rings. Fraudsters would order an item of jewellery online using stolen credit card details or a stolen identity. The jewellery would then be delivered to the fraudster at a holding address or intercepted during delivery. Obviously this causes a tremendous amount of stress for the individual whose card details or identity have been stolen. However, it also has a significant impact on the retailer. The money for the stolen item is generally refunded to the victim of the fraud by his or her bank. This lost revenue is then 'charged back' to the retailer via the bank.

To try to reduce the levels of fraud, suspicious transactions were investigated using a manual process, such as checking the electoral roll or phone directories. Unfortunately, this process could take weeks, leading to some genuine customers having to wait for their jewellery. When evaluating the process, Beaverbrooks clearly identified that they needed more robust and customer-friendly measures to tackle fraud.

To resolve the issue, Beaverbroooks' installed Authenticate Pro, an electronic identity checking tool, into their customer application form. Once the contact details for the order are submitted an identity check is performed. Data provided by the consumer is matched against information held on Experian's databases, flagging any suspicious activity that could indicate identity fraud, account takeover or a bogus delivery address. An approval decision is returned immediately, which gives Beaverbrooks confidence that the order is genuine.

Since implementing the software, Beaverbrooks has seen a reduction in online fraud. Customer service has also improved as Beaverbrooks is now able to confirm orders and ship goods much faster. As a result, repeat orders have increased.

YES!

If these examples are not enough to convince you of the danger of corporate identity fraud, you should also be aware that there are legal considerations to bear in mind: every organisation which has information about people in its records has a legal responsibility for that information. For example, under the Data Protection Act, an organisation may not discard intact customer, staff, and supplier information: it **must** be shredded or totally destroyed. Recently, The Financial Services Authority levied a £3.2 million fine on HSBC following the loss of unencrypted data by three divisions, so the message for any business, large or small, is clear: **protect your customer information or your reputation and your profits will suffer.**

Of course, depending on what type of company it is, the legal responsibilities differ, but no matter what it does, the organisation is obliged to be aware of what information it has, what the risks are in case of an information breach, and to take steps to deal with any breach. In other words, ignorance is no excuse in the eyes of the law: You need to know what data you have, what the risk is, and have concrete plans in place to mitigate it and to deal with any issues that arise if you want to avoid action from a wide range of independent bodies.

We live in an age when protecting information has never been so important. The cost of identity crime in the UK alone is estimated at £1.2 billion per annum and with the need to prove one's identity now being an essential part of our daily routine, there is an increasing risk of us all falling victim.

"It is believed that in the UK criminals earn £10 million a day from stealing personal information with a wide acceptance that this crime is an enabler for serious and organised criminals."

The impact of identity crime is more than just a monetary loss. Damage to credit rating following victimisation can prevent access to a whole range of financial services which can impact upon all areas of the victim's life. The business community has a responsibility to protect the personal information their customers provide them with as part of their operational procedures. The protection of our personal information is now a key responsibility across both private and public sector organisations. In 2007-8 there were 1,034 separate incidents of data loss in the UK. Of these losses, 80% involved the theft of personal information. The criminal is now shrewder in techniques for stealing our personal information. The activity of identity crime is no longer confined to so-called "bin raiding."

Assistant Chief Constable, Peter Lowton, the Association of Chief Police Officers lead on Identity Fraud, has the following advice. "It is as important to protect personal information in the online environment. As criminal techniques become more sophisticated so must the protection systems employed to protect our identities. We recommend that when using the Internet a security firewall is enabled to protect computers from viruses and cyber-attack. When using social networking sites, users should enable security options built-in to these sites and refrain from posting personal information. There is great commitment being demonstrated by Government and non-Government bodies, police forces, public and private organisations alike to work together to address identity crime. The Association of Chief Police Officers (ACPO) believes that by enforcing the law robustly, taking steps to prevent and disrupt criminal techniques and raising awareness at all levels of the need to actively protect our personal information, we will better protect ourselves and our communities from identity crime."

This guide for small businesses is another example of sound partnership work to prevent identity crime. ACPO is pleased to offer its support to this venture.

The next few pages give a quick summary of the Data Protection Act, PCI-DSS and the Companies House PROOF scheme to help give you a basic understanding of the legal obligations facing you and your business relating to the protection of information. On the last page of this guide, you will also find links to other useful organisations and information resources in the fight against corporate identity fraud.

DATA PROTECTION ACT

- **Requires anyone who handles personal information to comply with a number of important principles:**
  - Only hold information on individuals that is business-critical and that will be used for a clear, defined purpose; ensure those individuals understand that the company possesses this data and what it will be used for
  - Only pass on personal information with the individual's permission or reasonable expectation that this will be done
  - Hold all such information securely, granting access only to those in the organisation with a strict need to know. You must also ensure you keep information accurate and up to date
  - Delete or otherwise destroy personal information as soon as there is no more need for it
  - Ensure staff are trained in their duties and responsibilities under the Data Protection Act, and that they are putting them into practice
- *Further information at* **http://www.ico.gov.uk/what_we_cover/data_protection.aspx**

PCI-DSS

- The **Payment Card Industry Data Security Standard** (PCI-DSS) is a widely-accepted set of policies and procedures intended to optimise the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. It was created jointly in 2004 by Visa, MasterCard, Discover and American Express, and now includes JCB

- **Any company which stores, processes or transmits payment card data bearing the logo of the five major payment companies has to comply**
- Compliance is also required by any third party who accepts or processes payment cards, including call centres which receive cardholder data which they are unable to delete. If merchants use payment gateways to process transactions on their behalf, compliance is not required but they must ensure contractual obligation from the third party that they comply with PCI-DSS and are responsible for the security of cardholder data
- Fines for non-compliance or security breaches can be up to £500,000. In severe cases of non-compliance, the five major payment companies have threatened to remove the ability to process credit card payments, which could be economically fatal for any merchant

The PCI-DSS specifies and elaborates on six major objectives:

1. **A secure network** must be maintained for conducting transactions. This requirement involves the use of robust and specialised firewalls, authentication data such as PINs and passwords, which must not involve defaults supplied by vendors, and should be convenient for customers to change at any point
2. **Cardholder information** must be protected wherever it is stored. When cardholder data is transmitted through public networks, it must be encrypted in an effective way. Systems should be protected against hackers with frequently-updated anti-virus software, anti-spyware programmes, and other anti-malware solutions
3. **Access to information** and operations should be restricted and controlled; every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected electronically as well as physically (document shredders, avoidance of unnecessary paper document duplication, locks and chains on industrial bins)
4. **Networks** must be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-do-date
5. **A formal information security policy** must be defined, maintained, and followed at all times and by all participating entities. The policy also requires businesses to securely dispose of paper documents before disposal (*preferably using a cross-cut or high security shredder*) and to destroy any computer hard drives containing customer data (*shred, crush or degauss using DoD overwrite type processess*)
6. **Enforcement** measures such as audits and penalties for non-compliance may be necessary

Monitored, updated and promoted by the PCI Security Standards Council; further information at **www.pcisecuritystandards.org/security_standards/pci_dss.shtml**

SHOULD YOU BE WORRIED?

PROOF

Protected Online Filing **(PROOF)** is a service from Companies House that helps companies to protect themselves from being hijacked as it prevents individuals from filing certain paper forms. PROOF requires anyone who handles personal information to comply with a number of important principles and:

- Includes documents for an appointment/termination/change of particulars of company officers and change of registered office address
- When a company has joined the **PROOF** scheme, Companies House rejects any paper versions of these forms and sends them back to the registered office address, helping to ensure that any changes made have been registered with the company's authority
- **PROOF** is supported by Companies House's Web Filing Service and Software Filing services
- The former is an online registration service for the secure submission of company information; the latter requires the use of specialised software to file data with Companies House and is more appropriate for bulk users
- Both services require passwords, confidential authentication codes, and recognised email addresses

Further information at
www.ico.gov.uk/what_we_cover/data_protection.aspx

TRENDS IN FRAUD

Changing tactics

Many organisations are already responding to fraudulent activities by implementing sophisticated systems, so certain forms of business identity fraud are becoming harder for the fraudsters to achieve. Company impersonation, for example, was most commonly committed by fraudulently changing the legitimate company's registered address or director details filed at Companies House. However, changing a company's registered address or director details is no longer as easy as it once was for fraudsters. Businesses can now submit their documents electronically to Companies House, which has made the task more difficult and less susceptible to fraud.

Furthermore, with banks using authentication processes as part of their credit applications for businesses as well as individuals, it is harder for crooks to obtain credit in the name of a legitimate company. So why is identity fraud still a big issue? As with most things, fraud is evolving and some focus has turned to non-limited businesses and mail order or online suppliers.

Criminals have been stealing the identities of long established non-limited businesses, then targeting companies that are mail order or online based. These tend to be companies that trade in small, but high value items that can be sold on easily, such as electrical goods, laptops, satnavs, mobile phones, etc.

After placing high value orders in a legitimate non-limited business' name, the criminals direct the delivery to the trading address, which they had found in the public domain. They wait and intercept the delivery before disappearing with the goods. This could leave the non-limited business in dispute with the supplier over goods they never received. However, it could be months before the non-limited business even realises that it has been the victim of identity fraud – when the supplier chases payment or they receive a letter of court proceedings.

There are signs that small businesses can look out for and there are services that enable them to do this easily.

Keep an eye on:

- Any CCJs that appear on your records
- Any unusual payment activity
- Whether the number of suppliers on your payment records have increased
- Any changes to the director details
- Any changes to the proprietor details
- Any changes to the registered address
- Changes to your company credit score in all official company records and statements.

Vendor analyses of businesses have found that more businesses are beginning to see the benefits of monitoring themselves as well as businesses they trade with. However, many only realise the benefits after they have been the victims of fraud. For small businesses, one county court judgment could be the end of its trading days, so spotting the signs early is crucial.

National identity cards

Towards the end of 2009, anyone living in the Greater Manchester area who is already on the current passport register will be able to apply for an identity card. Identity cards will accompany the passport in providing a gold standard, Government-backed proof of identity.

The Greater Manchester launch is the first step in the countrywide roll-out of identity cards. The project will then open out to residents across the North West early next year, before identity cards are available nationwide by 2012.

As the roll-out begins, businesses and their employees need to be ready. From launch day the cards could be used anywhere in the UK, so anyone in a customer-facing role will need to know what to look for. The Identity and Passport Service (IPS) will be running an extensive public information campaign to make sure staff have all the information they will need to check whether an identity card is genuine. A Web site **www.businesslink.gov.uk/idsmart** has been set up to provide information to businesses on what ID cards will mean for them and to request point of sale materials.

There are three different types of identity card, two of which are being launched by IPS in 2009.

The identity card for British citizens is salmon and lilac in colour and features a passport-quality photograph of the holder as well as their name, date and place of birth, nationality and signature. The identification card for EU or European Economic Area citizens living in the UK is turquoise and green and holds all the same information, other than nationality.

Both cards feature the Royal Coat of Arms on the front and a laser-engraved floral pattern representing the shamrock, daffodil, thistle and rose on the reverse. This engraving is sensitive to the touch, and extremely difficult to forge. A chip inside the card will hold the same personal information electronically plus two fingerprints, securely locking in the individual's unique identity.

The identity card for Foreign Nationals was launched in 2008 by the United Kingdom Border Agency (UKBA) and further details are available from their Web site **www.ukba.homeoffice.gov.uk.**

For additional protection, and only with the customer's permission, registered businesses will be able to contact the dedicated IPS Card Validation Service (CVS) to check that the identity card is genuine and belongs to the customer presenting it. Identity cards therefore offer a more secure way to verify the identity of the person in front of you. The £30 cards may be used anywhere in the UK to prove age or identity and the identity card for British citizens could be used as a passport across Europe. Businesses will benefit from a new, highly secure proof of identity to help combat an ID fraud industry costing £1.2bn every year. Working with Government, businesses have a significant role to play in taking advantage of the very real benefits identity cards will provide. However, it is important to note that national identity cards will not solve the problem of identity fraud on their own. In order to be truly effective in the joint effort of fighting this crime, businesses and individuals must be vigilant in exercising a number of preventative and reactive measures. The outlines of several of these are given in the pages that follow, and further information can be found by visiting the links provided at the end of this guide.

The single-most important thing you can do to protect your business from identity fraud is to be aware of the risk.

Profile Technical Support Wakefield contacted the Yorkshire Chamber of Commerce after an employee was asked over the phone for the details of the owners of the company. The caller identified himself as representing the Yorkshire Chamber of Commerce and indicated that the Chamber wanted to send his company important information on EU Directives. When Mr. Cranswick asked why they hadn't sourced this information through Companies House, the caller promptly hung up. The Chamber confirmed it has made no such call so it seems likely this was an attempt by a fraudster to get access to information in order to begin corporate identity fraud. The lesson to learn (ably demonstrated by Mr. Cranswick) is never to give out any information about your company, your customers or yourself unless it is for a verified, valid reason and to a verified, legitimate organisation. Even more crucial is to make all staff follow this guideline too.

This example demonstrates the potential for loss from fraud in seemingly-innocuous, everyday business interactions. Just a few simple policy decisions can help a company protect itself against corporate identity fraud. Whether protecting your company from spying eyes or protecting people's privacy, creating an action plan for handling and disposing of important information are paramount to security. Businesses and organisations that don't have a plan in place are at risk, and the Government has introduced many regulations that affect most businesses today; under the Data Protection Act you could be fined if your business doesn't secure or dispose of confidential information correctly
(see pages 10-12 for more information).

Getting Started

Begin your policy by considering what type of sensitive information your company holds, where it is held and who has access to it.

You can classify this information into different levels as this may help make it easier for you to implement your policy:

- **General Information** (descriptive information or files with no customer or private details)
- **Sensitive Information** (contains customer or employee contact information or other details)
- **Confidential / Restricted Information** (contains financial information, bank account details or other information relating to your company's operating / products / management operation)

Files, folders and documents should be clearly labelled accordingly so it's easier for employee and employer to know who should have access to what, as well as where to store them when not in use and how to destroy them when they are no longer needed.

Review where sensitive and confidential/ restricted information is held and make sure this is in a secure place, separate from general, all-access information. Communicate clearly any new procedures to all staff, reminding and updating them regularly on these, and ensure that a named person is given the responsibility of checking that the system is implemented and followed by all.

Review who has access to each type of information and restrict it to only those who need to have it. Finally, review where information is kept when it is in use, when not in use but needed for legal or business purposes and what happens to it when you no longer need it. Don't forget things like uniforms, headed paper and even computers and disks when drawing up these lists – all can be used by fraudsters in some manner to carry out criminal activities in your company's name, so be sure to shred or otherwise destroy them completely.

Later in this guide you will find specific advice on a range of fraud prevention solutions, including protecting your company online, checking identities, and information destruction as well as an essential checklist at the end of this chapter (p22) to get you started.

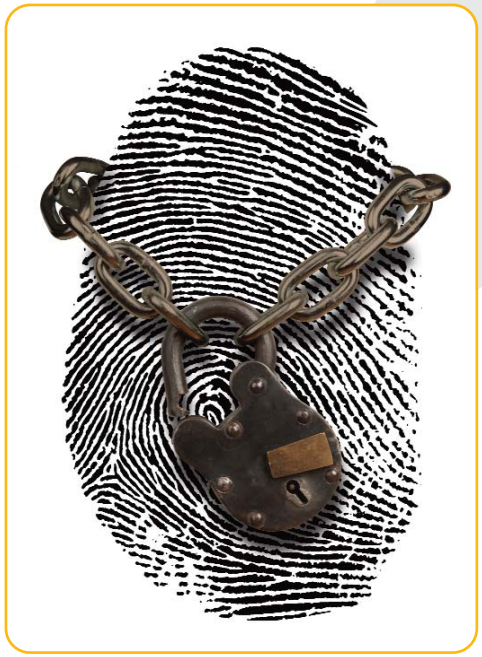
For more information, educational material and checklists, visit

www.stop-idfraud.co.uk/resourcecentre

or see the *Useful Contacts and Resources* section at the end of this guide.

WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

Don't take anything on face value



A more insidious threat to businesses is what is known as long firm fraud, where companies are incorporated and build up a good credit history for the sole purpose of then making multiple credit applications and defrauding their suppliers in the long-term. It's a waiting game for the fraudsters but one that can reap enormous benefits for them – and do serious damage to companies that have supplied services or products in good faith.

Arguably even more worrying is where a newly incorporated company files accounts at Companies House with facts too good to be true such as the turnover and profits earned by a new start-up in its first year of trading. The aim of this scam is to use the good credit rating thus obtained to buy goods on credit and disappear without paying. Again, businesses in the current economic climate are especially eager to secure new clients and this makes them particularly vulnerable.

The Commercial Fraud team at Equifax has seen an increasing prevalence of frauds being committed against small and medium sized businesses. Could this be one of the consequences of the recession? The heads of these businesses, already under increased financial pressure, have limited time to ensure they aren't falling foul of clever fraudsters. Unfortunately, the fraudsters know this and are making the most of the opportunity.

This guide has already looked at the most common types of fraud, but it's worth noting that (*in the case of company hijacking, for example*) damage to the credit status of a genuine company caused by fraudsters is especially worrying in the current climate where access to business funding is already limited.

Vigilance is key – not just of customers' data but your own company data at Companies House. Credit intelligence companies can help by keeping track of document filings and by monitoring customer credit activities to provide quick alerts if fraudulent documents are filed against a company. They can also interrogate their commercial databases for anomalies (e.g. unusual access patterns on particular company business credit reports that are out of keeping with previous access patterns or are from companies that operate in completely different business sectors).

At the end of the day, gaining as much intelligence about customers and suppliers as possible is a requirement, not a luxury: **don't take anything for granted.**

Identity Verification

Various documents can be used as a means of verifying a person's identity; for example, passports, driving licences, evidence of entitlement to a state or local authority funded benefit, current council tax demand letter or statement, current bank statements, or credit/debit card statements and utility bills. Documents such as passports, driving licences or identity cards contain a large number of security features. By contrast, utility bills do not usually contain any inherent security features. This, together with the easy access most people have to scanners, printers and software that can be used to manipulate images, means that they are relatively easy to forge. It's good practice to bear this in mind when being presented with such documents as part of a verification procedure.

The following is a brief outline of some of the techniques that can be used to verify identification securely:

Paper security features

- ***Ultraviolet (UV) light:*** When examined under UV light, most security papers are dull, whereas most commonly bought paper is bright. The difference can be easily seen by comparing a bank note with most office papers; original security papers are therefore likely to be dull, whereas forged ones will often be bright under UV light
- ***Watermarks:*** Are an integral part of security papers that contain them, produced during their manufacture. The only way to replicate a watermark is to print a pale image on the surface of the document. Such images are rarely as detailed or sharp as the genuine watermarks
- ***Fibres:*** Various lengths and colours of fibre may be added during the paper making process. These fibres may be visible to the naked eye or react under UV or infra-red light

Printing security features

- ***Commercially printed documents:*** Typically have good quality images in solid colours. Forged documents usually contain images made up of a series of dots using only three or four colours; the difference is usually obvious if genuine and forged document are directly compared, but a simple hand lens should enable the dots in a forged document to be seen
- ***Optically variable inks:*** Appear to change colour when viewed at differing angles. Currently there are only two types, green to purple and gold to green
- ***Microprinting:*** Extremely small text that appears as a continuous line to the naked eye, these characters cannot be replicated with a traditional colour copier or scanner
- ***Fluorescent Features:*** All security documents contain images that fluoresce under UV light. If attempts are made to replicate these features, they will rarely show the level of detail present in the genuine features

Other security features

- ***Perforations:*** Utility bills usually have a perforated portion. In forged documents the perforations may be absent or lack the crisp edges and regularity of genuine ones
- ***Spelling:*** Forged documents often contain misspellings or use different symbols from those on genuine documents
- ***Bank Stamps:*** Presence of a bank stamp does not prove authenticity since genuine stamps can be scanned and added to forgeries. However, there is an obvious difference between forgeries and originals when viewed with a hand lens (see commercially printed documents)

Signatures

- There are two main components to a signature, both of which need to be considered when determining whether a signature is genuine or forged:

- its pictorial appearance or shape

- its fluency *(the speed with which it is written)*

- Most forgers can only manage one of the two. A result of this is that complex, skilfully written signatures are much more difficult to forge than ones that are short and simply written

Identity verification is a highly-skilled process for which this subsection represents only a brief overview. When in any doubt, professional help should always be sought. Visit www.identitytheft.org for more information.

WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

Information destruction

Backing-Up Business and Customer Data

In the running of their day-to-day businesses, all companies naturally have to keep hold of certain confidential information on employees, customers and partners. It is good practice to conduct regular risk assessments on the security of this data, from the point that files are produced, through to the transit process and the ultimate place of their storage.

Companies should:

- Encrypt backed-up information that is held offsite (including while in transit)
- Carry out regular audits of encryption levels to ensure they match the current risk environment
- Backup any data being transferred by secure Internet links
- Ensure due diligence on third parties that handle backed-up information to achieve a comprehensive understanding of how it is secured, exactly who has access to it and how staff with access are vetted
- Provide employees with responsibility for holding backed-up data off-site with guidance on both personal and physical security
- Conduct spot checks to ensure information held off-site is done in accordance with accepted security policies and procedures
- Ensure that you have a properly tested business continuity plan

Disposal of Business and Customer Data

Once data being held is no longer needed, it should immediately and effectively be destroyed.

Companies should:

- Treat all paper generated as 'confidential' when no longer needed and ensure that is it disposed of securely, for example by using cross-cut or microshred shredders – don't throw any documentation away without destroying it first
- Always make sure you shred information before you leave your office or department. Don't assume other people will do it for you
- Regularly check general waste bins for the accidental disposal of confidential information
- Provide guidance for travelling or home-based staff on the secure disposal of company and customer data
- Implement a policy requiring that all electronic files be deleted as soon as they are redundant and that files transferred to portable devices be erased as soon as they have been used
- Ensure computer hard drives and portable media are properly wiped using specialist software or destroyed as soon as they become obsolete
- Check how third parties vet their staff and audit their adherence to waste disposal procedures and best practice guidelines. If you use a third party supplier to destroy electronic equipment or corporate uniforms for example, make sure they have BSIA Accreditation
- Ensure that all members of staff are aware of, and sign up to, the policy
- Operate a zero tolerance policy with staff that flout company policy and / or compromise the safety and security of data

Online security - keeping your information safe

One of the keys to business continuity and protection against fraud is to keep all critical and sensitive information safe from potential spyware, malware and spam threats. Small businesses need a reliable, cost-effective and hassle-free way to make sure their important data is always available. Achieving this takes more than an anti-virus solution.

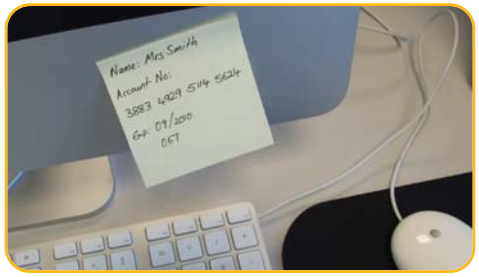
Security threats are increasing in complexity, number, and frequency and many are now designed to target specific information while also evading detection by a single security mechanism such as anti-virus software. Moreover, many of today's attacks do not discriminate based on the size of the company. The volume of information small businesses must protect continues to expand and thus the small business is coming to a crossroads where it has to strengthen its IT security but may not know how to do so.

One of the best and most cost-effective solutions to this problem is an all-in-one security product that tightly integrates solutions to protect against multiple threats at multiple points and can be easily managed and controlled from a single intuitive console. True protection must be comprehensive, including threat protection and backup and recovery.

Threat Protection: Current malware quietly exploits vulnerabilities or weaknesses in applications and systems to make its entry into the corporation silent and easy, thereby increasing the likelihood that an attack will go undetected just long enough for the attacker to find and steal valuable sensitive information. *Protecting against such a vast range of threats requires a combination of security measures, including anti-virus, firewall(s), anti-spyware, intrusion prevention and anti-spam to thwart these 'noiseless' threats.*

Backup & Recovery: Statistics from Symantec show that half of small businesses have lost important data from their computers. This highlights a serious concern: how to ensure backup practices are keeping pace with information protection requirements. A truly effective security solution needs to be able to address lost data concerns by providing backup and recovery capabilities, and many such solutions are offered online and are automated, continuous, secure, and reliable.

A multifaceted all-in-one security suite will allow small enterprises to protect and enhance their businesses. By leveraging such technology, small businesses can keep their critical and sensitive data safe from increasingly sophisticated threats while keeping data available and protected.



WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

End-to-end protection: Any solution must be sophisticated enough to defeat not only known, but unknown threats. SMEs need to know that their critical information is safe, wherever it's used or stored (laptops, desktops, mobile devices, servers, in email, over the network, and in storage devices).

Effective and accurate anti-spam protection: Is especially urgent given Symantec's observation last year of a 192% increase in spam across the Internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008. Recently, cyber-criminals capitalised on fears of the "swine flu" to attack users, at one point sending approximately 1 billion flu-related messages a day. SMEs require a solution that automatically detects spam without requiring manual adjustment of filtering rules or monitoring of false positives.

Rapid, reliable backup and recovery: Ensuring that data and the systems it resides on are secure, backed up, and able to be recovered quickly is essential. SMEs need to easily restore data or systems and protect against new threats through automated, event-driven backups. Downtime must be minimised, so users can recover individual files and folders in seconds, or complete Windows systems in minutes.

Simplified management: For SMEs, simplicity is a significant priority since most don't have the staff or the in-house expertise to spend time managing security. Solutions must be deployed with minimal disruption to business operations.

CHECKLIST

DO:

- Develop an anti-fraud policy statement and clearly communicate it to all employees
- Ensure that checks are carried out on all new employees (and all those with access to the building, such as cleaning staff) including references, qualifications, experience and past employment and verification of identity
- Securely destroy all documents containing confidential or sensitive business information before disposing of them using a cross-cut or microshred shredder. Make sure you do this before you leave your department or office
- Store confidential or sensitive information in a secure place and limit access
- Check your business's registered details at Companies House on a regular basis
- Register for Companies House PROOF scheme and monitor service
- Review your credit report on a regular basis
- Include fraud prevention and detection within your induction programme for all new employees and provide ongoing fraud awareness training to all employees
- Undertake checks on all new customers and review existing customers on a regular basis
- Implement a clear desk policy
- Encourage a 'no blame' culture where security issues can be discussed without recrimination before transgressions occur
- Introduce a whistle-blowing policy and clearly communicate it to all employees
- Ensure your IT security policy covers mobile devices, laptop computers, the Internet and email. Review it on a regular basis

DON'T:

- Assume that the information provided by prospective employees is accurate: Independently verify it
- Give employees unlimited access to sensitive or confidential information unless it is necessary
- Rely solely on information obtained from Companies House when checking a new customer's credit history; use other credible sources
- Put business bank account details and directors' signatures into the public domain (e.g. on your Web site, or send to anyone via unencrypted email)
- Use default or obvious passwords and make sure your staff don't either
- Throw unwanted papers in the bin – shred them first, including abandoned or cancelled receipts, DVDs and CDs. When disposing of old uniforms or corporate clothing make sure these are destroyed properly so that no one else can use them
- Throw away an old computer or laptop without wiping clean the hard drive first
- Leave documents in meeting rooms or on top of printers
- Give out any information about your company, your customers or yourself unless it is for a valid reason and to a legitimate organisation – make sure all your staff are aware of this and all the steps included in this checklist

WHAT TO DO IF YOUR BUSINESS BECOMES A VICTIM

Corporate identity fraud can have a financial and reputational impact on your organisation. You will need to rectify the damage caused by the fraudster (especially to your credit rating) and this can take time.

According to the Federation of Small Businesses, 33% of small businesses who had experienced fraud did not report it, the prevailing attitude seeming to be that doing so would not accomplish anything. A significant minority, however (7%), indicated that they were not sure how to report it or who to contact. More shockingly, several businesses when asked to comment further said they would not report viruses or phishing emails because they are seen as very common and therefore, presumably, unworthy of calling to the attention of the relevant authorities. In some cases, affected companies only became aware of the fraud after being contacted by their bank.

This reluctance to report fraud crimes plays directly into the criminals' hands. There are many different institutions that can help track down and punish fraudsters, and at the very least there is an obligation to notify customers, partners and suppliers of possible security breaches. When crimes are left unreported, however, the criminals survive to attack other organisations and individuals, all the while becoming more sophisticated in their approaches. Unfortunately, 97% of businesses said that they were not a member of a regional fraud forum, an incredible 90% said that they have never heard of them, and 15% claimed they were not sure there was any benefit to their business in belonging to one. Clearly, there is an onus on such forums to reach out more effectively to small businesses and specifically target them with accessible information about prevention, but equally a business must be aware of the dangers and report incursions. It is, after all, a legal responsibility.

FIVE STEPS YOU SHOULD TAKE:

1. Report the matter to the police and other relevant organisations immediately (e.g. suppliers, Companies House). Follow their advice
2. Inform your customers if their details may have been compromised or a fraudster may have contacted them as a 'representative' of your business
3. Obtain copies of your organisation's credit report and Companies House record and check for discrepancies. Go back to step 1
4. Keep a record of all correspondence you make or receive in respect of the corporate identity fraud
5. Reassess your organisation's risk management and control systems to ensure that your business is adequately protected

Legal recourse

Criminal prosecution: Corporate identity fraud is a criminal offence and the police will consider taking criminal action if you refer the matter to them promptly.

Civil recovery: An alternative to criminal prosecution which may enable your business to recover some of its stolen assets. You should seek legal advice.

In both cases, do look at the links provided on the final page of this document for further information.

WHAT CAN YOU DO TO PROTECT YOUR OWN IDENTITY?

Many of the lessons learned in preventing corporate identity fraud are equally applicable to you as an individual. First and foremost, it's important to be aware that there is a risk and to identify which areas of your life it applies.

A common error is to assume that the technology we use is solely responsible for protecting our identities, and that it is, in some ill-conceived way, infallible. Yes, we have virus protection and spam filters, but that does not mean we should open emailed files from unknown senders, nor assume that an email passing the spam filter is legitimate – it may sound obvious, but tens of thousands do this every day. We all receive papers and files on a daily basis which contain sensitive information about us or our family. To us, they are just records of our lives and transactions, to a fraudster they could be the key to stealing our identities. For example, a combination of the following could be enough to help somebody steal your identity:

- Utility Bills, bank and credit card statements – not forgetting the cards themselves once they have expired
- Copies of your passport or driving licence
- Anything with your home address, most especially if it has customer reference numbers or similar data on it
- CVs, job application forms, copies of your (or your original) passport, driving licence or workplace identity cards - even if they are out of date

By going back to basics when considering disposing of or sending out this information, a large portion of risk can be averted. With respect to physical documents, cards or even corporate clothing, a general rule of thumb should be: **if in doubt, destroy it.**

Below are some more tips for individuals to consider, many of which apply equally well to your behaviour at work:

- **Beware of anybody who contacts you** unexpectedly and asks for personal information or account details even if they claim to be from your bank, the police or another official organisation like your local council. Ask for their name and a contact number and then check with the organisation in question before calling back
- **Pay attention to billing cycles** - Contact creditors immediately if your bills arrive late. A missing bill could mean a fraudster has taken over your credit card account and changed your billing address
- **Shred old documents and disks/CDs** before disposing of them (preferably with a cross-cut shredder) to make sure they are truly undecipherable before discarding. Tearing a document into large pieces or shredding into vertical strips is not enough: If you can reassemble the item in question, so can anyone else. Do you recycle? The system works just as well with shredded papers as non-shredded, and recycling bins could be an easy target if you are throwing away your papers intact
- **If following a link from an email,** never input personal data into the Web site. If you think it might be genuine, close your browser, reopen it and see if you can navigate to the same page from the organisation's homepage. Similarly, never give out your full details over the phone if called proactively by for example, your bank. Call them back on their listed number (not the one they give you on the phone) and find out if the call was genuine

WHAT CAN YOU DO TO PROTECT YOUR OWN IDENTITY?

- **Don't reuse passwords** for different Web sites and organisations but vary them, and make them as complicated as you can remember. Change them regularly. The same applies to social networking sites like Facebook
- **If you use the Internet** make sure you have the latest security patches and up-to-date anti-virus software installed. If you use social networking sites always use the privacy settings available and be wary of posting personal information which people you don't know can gain access to
- **Fraudsters may try to redirect your mail** without your permission. If you suspect your mail is being stolen or a mail redirection application has been made in your name without your knowledge contact ***Royal Mail Customer Care on 08457 740 740***.
- **If you move house**, tell your bank, card issuer and of course all other organisations that you deal with immediately, but don't forget to ask Royal Mail to redirect any mail from your old address to your new one for at least a year

These may seem like simple steps, but they're important and effective and, unfortunately, ignored by far too many people: **don't make it easy for fraudsters.**

For more information on how identity crimes occur and on how to protect yourself and your family, visit **www.stop-idfraud.co.uk**

CASE STUDY: Marc Whiteley

Marc Whiteley, 22, an assistant manager with a financial institution in Manchester, never gave much thought to identity fraud until he received an email last November from Alliance & Leicester telling him that his 'application for a credit card was being processed'. Marc hadn't applied for a credit card so he contacted A&L, who immediately cancelled the application. Unfortunately the criminal - who had got hold of Marc's date of birth, email and postal addresses among other bits of key information, such as his salary – had applied for other loans and cards and Marc continued to receive emails alerting him to new applications under his name.

Concerned, Marc contacted the police but was still extremely worried about the extent of the criminal's activity under his name and how this could affect his credit score as he had been planning to get a loan to buy a new car. It was also time consuming and extremely frustrating dealing with lenders individually to try and cancel each application and get removed from their records.

At this point Marc saw an advert for a credit reference agency and joined immediately to check his credit report. Once registered, Marc found a further five applications in his name that were fraudulent. The Victims of Fraud team at Experian stepped in to help Marc, and a note was attached to his credit report explaining that he had been the victim of attempted ID fraud. Enquiries were then launched with each of the organisations involved to help Marc recover his identity and rectify his credit report as soon as possible. Marc was given regular progress reports until the matter was fully resolved.

Marc said, "It was a huge relief. Before this happened I never thought twice about ID fraud and certainly didn't think I'd end up becoming a victim of it. I'm now extremely vigilant about getting rid of my confidential information to make sure that it's not out there for criminals to exploit and I check my credit report every week to make sure no further applications have been made in my name fraudulently. It may seem like a chore at the time but having these simple processes in place will hopefully save a lot of hassle and heartache down the line."

Recent research by CreditExpert found that almost two thirds (63%) of victims of identity fraud discovered they had become a victim by noticing fraudulent activity on their credit report, while 15% of victims discovered their identity had been compromised after being contacted by a financial services company. Safeguarding all your private information and monitoring your credit report helps to ensure you are one step ahead of fraudsters.

AFTERWORD

Dr Bernard Herdan
CEO
National Fraud Authority

"Identity (ID) crime and related fraud can impact on so many aspects of a small business. From financial loss, through to the effects it can have on customers, investors, staff and corporate reputation – the consequences can be devastating.

In addition to this, the theft of an identity can also underpin a range of other serious crimes. It can be used to conceal criminal identities so organised gangs avoid detection. It can facilitate terrorism, human trafficking and the illegal drugs trade.

Working with over 400 stakeholder organisations, the National Fraud Authority is tackling fraud from a strategic viewpoint. We recently conducted a review of ID crime which assessed the national response to the problem. The analysis identified gaps where fraudsters exploit the system and we are now working with our stakeholders to close off these opportunities.

The review has led to the launch of the ID Fraud Taskforce, which is targeting the criminal production and misuse of both forged and genuine documents while also looking at ways to stop criminals from obtaining documents fraudulently.

The UK's first National Fraud Reporting Centre (NFRC) will help streamline fraud reporting while also building a more robust intelligence picture through the National Fraud Intelligence Bureau. This information will help predict fraud trends and geographic fraud 'hot spots', and will potentially help protect everyone from fraud in the future. The NFRC will also give advice to fraud victims who contact it on how to prevent themselves from becoming repeat victims.

However, there is only so much to be gained from reporting a fraud after the fact. Ideally, preventing fraud should always be the main focus. I encourage you to take the time to read this guide and adopt the simple suggestions that will help prevent your business from becoming a victim of ID crime.

Often the only investment required is your time. Raising staff awareness, regularly changing passwords or the introduction of a document handling policy can sometimes make a critical difference.

Please use the guidance above to 'fraud-proof' your business and prevent criminals from stealing your corporate identity and damaging your business."

ABOUT THIS GUIDE

Mind Your Own Business - A Practical Guide to Identity Fraud Prevention For Business was produced by Fellowes (www.fellowes.co.uk) on behalf of and in conjunction with its associate organisers of National Identity Fraud Prevention Week 2009. It is intended to be used as an introductory guide to the common types of corporate identity fraud and the risks they pose, as well as to provide practical pointers on protecting small businesses in Europe and a list of useful resources for those seeking further information.

Special thanks are due to the following people and organisations for additional content:

- David Lennox, head of policy and projects, CIFAS (www.cifas.org.uk)
- Ross Walker, head of small and medium business, Symantec UK & Ireland (www.symantec.co.uk)
- ACC Peter Lowton, ACPO Lead on Identity Crime and The National Identity Scheme, ACPO (Association of Chief Police Officers) (www.acpo.police.uk)
- James Blake, head of UK identity authentication, Experian (www.experian.co.uk)
- Kevin Burt, Identity Crime Policy Officer, Identity and Passport Service (www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/index.htm)
- Neil Munroe, External Affairs Director, Equifax (www.equifax.co.uk)

National Identity Fraud Prevention Week 2009 is supported by Fellowes, the Metropolitan Police, the National Fraud Authority, the Federation of Small Businesses, Equifax, CIFAS - The UK's Fraud Prevention Service, Callcredit, Experian, the Association of Chief Police Officers, the Home Office's Identity and Passport Service, the British Chambers of Commerce, the British Retail Consortium and the Royal Mail.

USEFUL CONTACTS AND RESOURCES

Further information

www.stop-idfraud.co.uk is a fraud prevention Web site that contains useful information on the types of fraud your business may be vulnerable to, as well as how to protect your business against fraud and further advice on what to do and who to contact should you become a victim. The Web site has been launched as part of **National Identity Fraud Prevention Week 2009**.

Visit the Web site to download free templates, checklists and support materials as well as to find out more information on identity fraud.

Additional information on corporate and personal identity fraud can be found at the following locations:

- Business Crime Reduction Centre: www.bcrc-uk.org
- Callcredit Ltd: www.callcredit.co.uk
- CIFAS – the UK's Fraud Prevention Service: www.cifas.org.uk
- City of London Police Fraud Desk: frauddesk@cityoflondon.pnn.police.uk
- Companies House: www.companieshouse.gov.uk
- Equifax Plc: www.equifax.co.uk
- Experian Ltd: www.experian.co.uk
- Fellowes: www.fellowes.com (Freephone 00 800 1810 1810)
- Fraud Advisory Panel: www.fraudadvisorypanel.org
- Home Office Identity Fraud Communication Awareness Group: www.identitytheft.org.uk
- Identity and Passport Service: www.ips.gov.uk
- National Fraud Authority: www.attorneygeneral.gov.uk/nfa
- The Federation of Small Businesses: www.fsb.org.uk/
- www.getsafeonline.org
- www.banksafeonline.org
- www.cardwatch.org.uk
- www.becardsmart.org.uk
- www.fraudadvisorypanel.org
- www.keepyour.co.uk
- www.met.police.uk

Local Fraud Forums

- www.northeastfraudforum.co.uk
- www.midlandsfraudforum.co.uk
- www.southwestfraudforum.co.uk
- www.northwestfraudforum.co.uk
- www.easternfraudforum.co.uk
- www.eastscotlandfraudforum.org.uk
- www.yhff.co.uk

Guide kindly produced by Fellowes, 2009