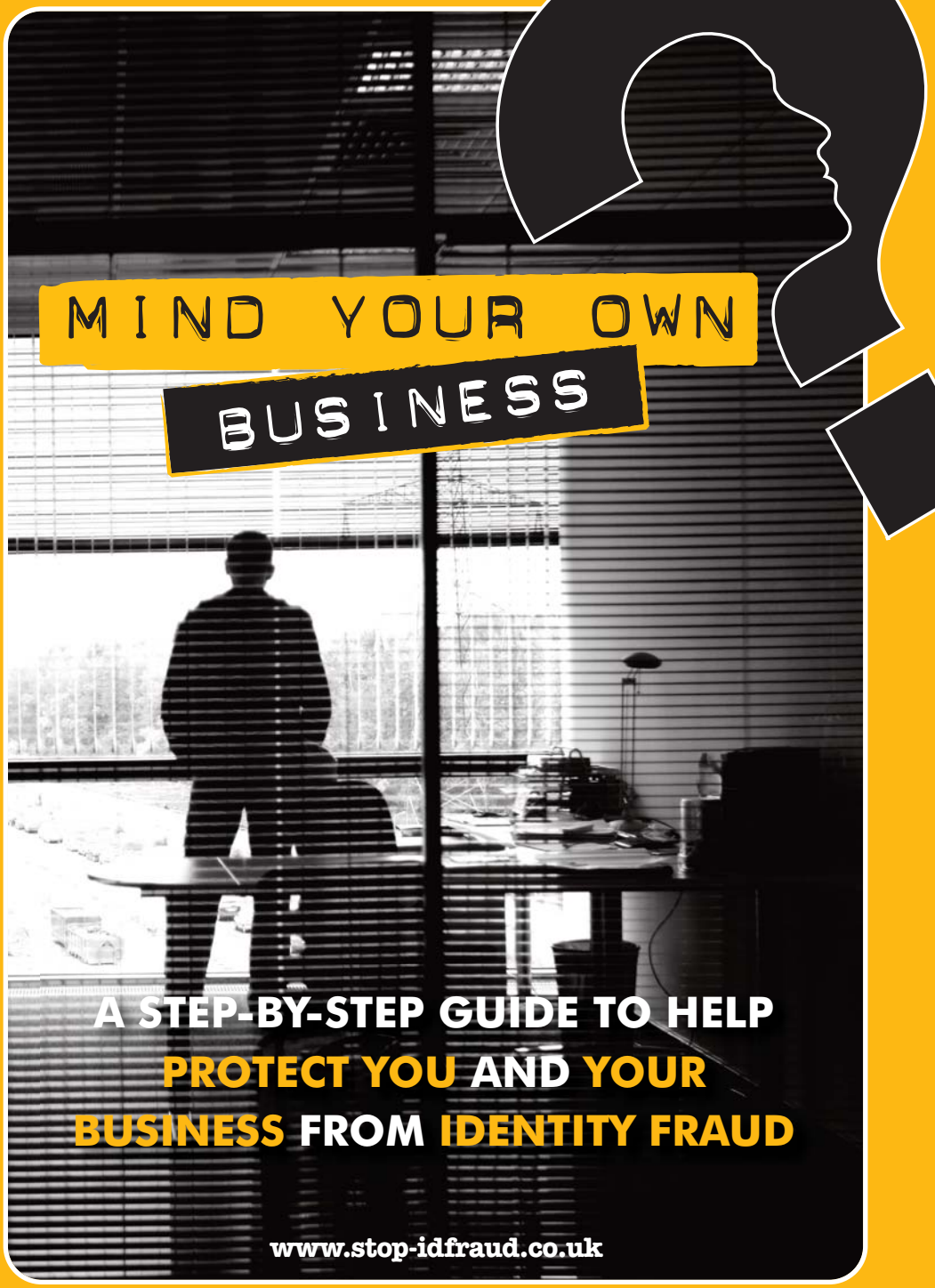


MIND YOUR OWN BUSINESS

A STEP-BY-STEP GUIDE TO HELP PROTECT YOU AND YOUR BUSINESS FROM IDENTITY FRAUD

www.stop-idfraud.co.uk

FOREWORD

NATIONAL IDENTITY FRAUD PREVENTION WEEK BUSINESS GUIDE 2010

Ann Swain

Home Affairs Chairperson

Federation of Small Businesses

"Recent FSB research shows that 5% of businesses have been victims of company identity fraud in some form[1]. While some may think that 5% 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 many different ways, including online, and businesses need to be on their guard to protect their sensitive business data, and that of their staff, customers and clients.

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. Protecting online information on customers and clients is even more important with the introduction of a huge £500,000 fine for businesses guilty of serious breaches of the Data Protection Act. A measure to concentrate minds if ever there was one!

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 as and when it happens to improve the picture of fraud in the UK and inform targeted investigations. Action Fraud (www.actionfraud.org.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. If immediate police intervention is required, also contact the police. 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."

You can visit www.stop-idfraud.co.uk to find additional information about how to protect yourself and your business against identity fraud.

[1] FSB 'Voice of Small Business' Survey Panel (June 2010)

CONTENTS

1. OVERVIEW AND FAST FACTS

Identity fraud is not someone else's problem. Everyone is vulnerable to identity fraud, even if they're not aware of it. This especially applies to companies. Personal identity fraud is frequently in the news but corporate identity fraud is often overlooked as many companies have the illusion of being safe or simply don't report it. Companies can become vulnerable to having their identities stolen in a variety of ways, both through internal and external routes, yet many companies do not take these into consideration. The impact of fraud on a commercial organisation (whether it is fraudulent customers or suppliers who steal goods, money or services by using a false identity, or a fraudster stealing a company's own identity) can be significant, causing considerable harm to a company's credit rating, reputation and ultimately, profitability.

Identity fraud can also have wider implications for a company. Firms can unwittingly cause third parties such as employees or customers to become victims of identity fraud through information breaches. A survey carried out for National Identity Fraud Prevention Week revealed that 82% of British people admit the identities of employees and/or customers of the companies they work for could be at risk of being acquired by an identity fraudster.

However, there are ways to reduce a company's vulnerability to identity fraud. Very simple steps such as shredding sensitive documents or having a comprehensive document policy can massively reduce the likelihood of identity thieves getting hold of sensitive data. This guide has been produced in an effort to show businesses how easily they can protect themselves from identity fraud and how vital it is.

This guide is aimed at providing the basic facts to help businesses in the ongoing battle against corporate identity fraud.

- 36% of businesses don't have a comprehensive policy or procedure in place to help prevent identity fraud[2]
  (See section 5.1 to find out how you can develop a policy for your business)
- 94% of British employees consider themselves to be at risk from identity fraud
- Only 56% of businesses have put in place a clear policy on how to handle documents with sensitive information[3]
  (See section 5.4 for tips on information destruction)
- Only 7% of consumers feel totally confident that their personal data is being handled securely by businesses[4]
- Under the Data Protection Act, an organisation should not discard intact customer, staff, and supplier information: it must be securely destroyed; not doing so could result in a £500,000 fine[5]
- Damage to an organisation's credit rating as a result of identity theft or fraud can prevent access to a whole range of financial services, ultimately impacting on its on-going operations
- One third of employees are still throwing away documents without shredding them first[6]
- Overall, 71% of UK employees think their companies should do more to ensure confidential documents are handled responsibly[7]

[2] A report by Fellowes for National Identity Fraud Prevention Week 2010 [3] A report by Fellowes for National Identity Fraud Prevention Week 2010 [4] A report by Fellowes for National Identity Fraud Prevention Week 2010 [5] Data Protection Act [6] A report by Fellowes for National Identity Fraud Prevention Week 2009 [7] A report by Fellowes for National Identity Fraud Prevention Week 2009

2. IDENTITY FRAUD RISKS TO YOUR BUSINESS

SECTION 2 OBJECTIVES:

- **Understand how identity fraud can impact your business**
- **Learn more about the types of identity crime**
- **Get an insight into how fraudsters work**

The term 'corporate identity fraud' refers to the impersonation of an organisation for financial or commercial gain. Some of the most common forms of fraud are:

Information Breaches: They occur when a business does not protect sensitive information like financial statements, employee records and contact details, and this information falls into the wrong hands. This is an extremely serious source of fraud and negligence in this area can result in significant fines. *(See section 3 for fines that companies can be liable to.)*

Company Identity Fraud: When a fraudster submits false documents to Companies House and changes the registered address of an organisation, often including appointing 'bogus' directors. Alternatively, a fraudster may simply set up a false company to purchase goods and services on credit and disappear before paying for them. Organisations can be vulnerable to corporate identity fraud committed internally by employees or externally by individuals or organised criminal gangs.

Impersonation: The fraudster impersonates a business to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them, for instance by using a 'phishing' email. 'Phishing' scams are when personal or business banking details are obtained through emails or fake web pages.

Impersonation can also happen when high value orders are placed in a legitimate non-limited business name and delivery is directed to the trading address. The fraudsters already have this address, available publicly, so they await delivery and intercept the goods when they arrive, then disappear. This could leave the non-limited business in dispute with the supplier over goods they never received let alone ordered.

Company Hijacking: Long-established and well-run companies are targeted by fraudsters who literally 'hijack' the company by investing in the business and appointing a member of the syndicate to the board of directors, where they wield influence.

Fraudulent Customers: Customers who 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.

2. IDENTITY FRAUD RISKS TO YOUR BUSINESS

Fraudulent Suppliers: Fraudsters set up a fake company (at varying levels of sophistication) and obtain payment for products or services which then never appear.

Long Firm Fraud: Companies are incorporated and build up a good credit rating for the sole purpose of then making multiple credit applications and defrauding their suppliers in the long term.

Short Firm Fraud: This is similar to long firm fraud but it takes place over a much shorter timescale. Usually, the business doesn't try to establish any form of credit history or credibility, apart from perhaps filing false accounts at Companies House if it's a limited company.

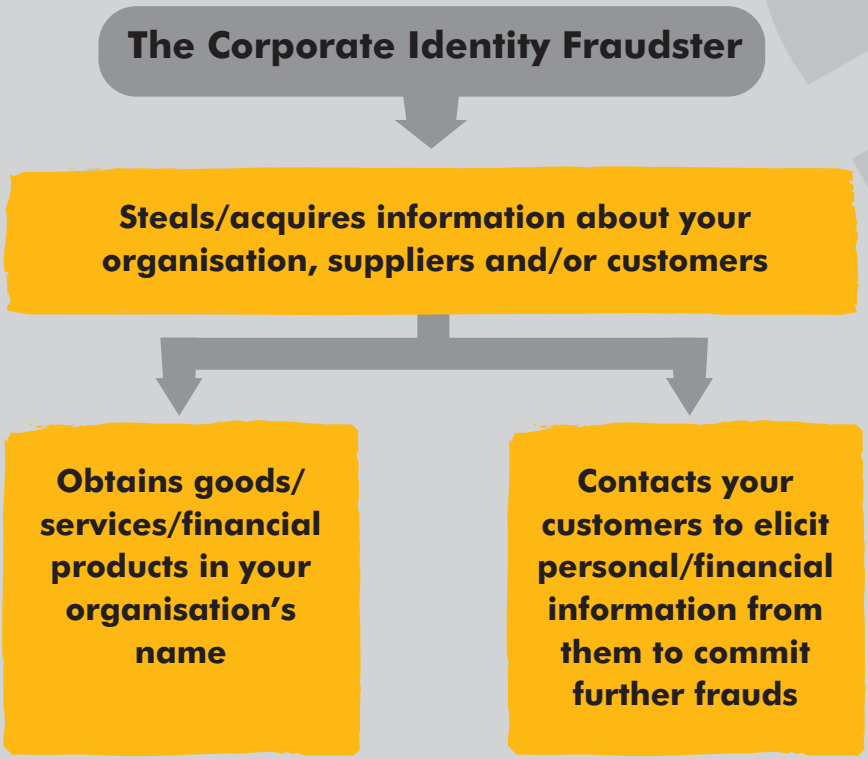
The fraudulent business has no day-to-day trading activity. Instead, the fraudsters use credit to obtain goods that are delivered to third-party addresses, often on multi-occupancy trading estates. Again, the goods are sold on for cash and the criminals then disappear.

Newly-Incorporated Companies: Newly-incorporated companies are not required to file accounts until up to 19 months of trading so in this scam the fraudster will file bogus accounts at Companies House showing exaggerated levels of revenue and profits during the first year of trading. The aim is to use the resulting good credit history to buy goods on credit and disappear.

Phoenix Companies: A director, or directors, set up a business which subsequently fails owing substantial amounts of money. The directors then create another company operating in the same field, often using a similar or even the same company name. Creditors of the original company lose out when the company goes bust. The directors have no financial responsibility to settle the debts and they can start again with no negative impact.

Fraudsters seek to acquire or steal the following types of information:

- 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 and suppliers
  - purchase assets



Source: the Fraud Advisory Panel

Case study: 'Beaverbrooks'

"It happened to my company"

In 2001, Beaverbrooks launched its website, 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 website became a prime target for fraudsters.

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. Although this caused a tremendous amount of stress for the card holder whose details had been stolen, 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 and 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, Beaverbrooks embedded an electronic identity checking tool into its customer application form. Once the contact details for the order are submitted, an identity check is performed by matching data provided by the consumer against information held on a database, which flags 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.

3. DATA PROTECTION AND THE LAW

SECTION 3 OBJECTIVES:

Discover the legal obligations facing companies;

- **Data Protection Act – This requires anyone who handles personal information to comply with a number of important principles**
- **Other possible fines – Some possible fines companies could face if they do not take data security seriously**
- **PCI-DSS – Details of the Payment Card Industry Data Security Standard**

Below is a quick summary of the Data Protection Act and 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. Additional information can be found in section 11 of this guide.

3.1 **DATA PROTECTION ACT**

- Requires anyone who handles personal information to comply with a number of important principles, including:
  - 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
  - Hold all such information securely, granting access to only those in the organisation with a strict need to know; keep this access list 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
- Under the Data Protection Act, an organisation should not discard intact customer, staff, and supplier information: it must be securely destroyed
- Further information at http://www.ico.gov.uk/what_we_cover/data_protection.aspx

3.2 **OTHER POSSIBLE FINES APPLICABLE TO NEGLIGENT COMPANIES**

- The UK Financial Services Authority is able to give companies fines if they allow data breaches. Last year the FSA fined HSBC £3,185,000 for losing its customers' data.
- The **Information Commissioner's Office (ICO)** is able to issue fines of up to £500,000 for serious breaches, as well as enabling it to conduct compulsory audits in central government departments where breaches may have occurred.

3.3 **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 by the five major credit card companies (Visa, MasterCard, Discover, American Express and JCB).
- It applies to any company which stores, processes, or transmits payment card data from these companies or any third party who accepts or processes payment cards.
- 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 or the loss of rights to use credit card payments.

Further information can be found at the PCI Security Standards Council website at:
http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

4. TRENDS IN FRAUD

SECTION 4 OBJECTIVES:

- **Look at the emerging trends in identity fraud and the geographical and demographic impact.**
- **Find out what signs to look out for on official company records to avoid corporate identity fraud**

In the UK, London remains the overall fraud hotspot, followed by St Albans, Guildford and Epsom. Geographically the South of England is more at risk than the North.[8]

Small and medium size businesses can often be targets for identity fraud, especially company hijacking, long firm fraud and fraud by newly-incorporated companies (see section 2). While firms have a good awareness of how financial fraud might affect a business, there is a lack of awareness of the risks of online fraud and company identity fraud.[9]

Fraudsters can also impersonate non-limited businesses and target mail order or online suppliers that trade in small but high value items that can be sold on easily, such as electrical goods, laptops, satnavs, mobile phones etc.

There are signs that small businesses can look out for to avoid corporate identity fraud and services they can use to support them. It is crucial to monitor all official company records and statements for:

- any CCJs that appear on your records
- any unusual payment activity
- whether the number of suppliers on your payment records has increased
- any changes to the director details
- any changes to the proprietor details
- any changes to the registered address
- any changes to your company credit score

Vendor analysis has found that more businesses are beginning to see the benefits of monitoring themselves as well as the businesses they trade with, before becoming victims, since one county court judgment could mean the end of a company's trading days. Only 56% of businesses have put in place a clear policy on how to handle sensitive information, so vigilance and spotting the signs early are key.

Fraud can be as complex as described above but paper-based fraud is also a challenge. 35% of employees admit to not shredding all high-risk documents before disposing of them. Additionally, 93% of employees believe that their company does not protect customers' identities sufficiently. Paper-based fraud can be easily prevented but employees need the tools and information to act appropriately.

[8] Experian 'The Insight Report' [9] Equifax 'Fraud Risks to Business Survey'

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

SECTION 5 OBJECTIVES:

Examine the practical ways in which companies can protect themselves against identity fraud;

- **How to create your own anti-fraud policy –** Steps to help you guard against the threat of identity fraud
- **Authentication –** How to authenticate and verify customers' and suppliers' identities
- **Identity verification –** Tips to verify an individual's identity
- **Credit checks –** How to carry out a credit check on an individual or business
- **PROOF –** A summary of the Companies House service that helps companies to protect themselves from being hijacked
- **Information destruction –** A guide to the back-up and destruction of sensitive data
- **Online security –** A guide to the measures to take to prevent e-crime
- **Checklist –** The essential do's and don'ts of preventing identity fraud

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

5.1 **HOW TO CREATE YOUR OWN ANTI-FRAUD POLICY**

The single-most important thing you can do to protect your business from identity fraud is to be aware of the risk. Then, just a few simple policy decisions and an action plan can help a company protect itself against corporate identity fraud. In addition to the steps below, in order to have a comprehensive policy in place, every company should undertake customer and supplier authentication, identity verification, information destruction and online security measures detailed in this chapter.

STEP 1 - Consider 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 operations or to your customers

STEP 2 - 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 securely when they are no longer needed.

STEP 3 - Review where sensitive and confidential/restricted information is held and make sure this is in a secure place, separate from general, all-access information. 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.

STEP 4 - Review who has access to each type of information and restrict it to those who truly need it. Communicate clearly any new procedures to all staff, and ensure that a named person is given the responsibility of checking that the system is implemented and followed by all.

STEP 5 - 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.

For more information, educational material and checklists, visit www.stop-idfraud.co.uk/resourcecentre or **see *section 11*** at the end of this guide.

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

- Only 56% of British organisations have a comprehensive policy to help protect people's identities.
- Over 60% of British people think their organisation should be doing more to ensure the secure handling of confidential documents.
- 93% of people are not completely confident that the organisations they deal with treat their personal information in such a way that it will not accidentally fall into the hands of identity fraudsters.
- 82% of British people admit the identities of employees and/or customers of the companies they work for could be at risk of being acquired by ID fraudsters[10].

5.2 **AUTHENTICATION - A KEY PRACTICE FOR BUSINESS**

The ability to authenticate and verify customers' identities is integral for any business that is serious about protecting itself against identity fraud. It is critical that companies take prudent steps to ensure that they know who they are doing business with when dealing with customers or suppliers. Failure to do so can result in businesses losing substantial amounts of money, damage to reputation and in some instances bankruptcy and closure.

The National Fraud Authority has produced a good practice guide to identity authentication and verification. This provides a step-by-step process and set of guidelines on how businesses can authenticate and/or verify the identity of their customers with a comfortable degree of assurance.

Below are some of the steps you can follow to protect your business from 'Card Not Present' fraud:

1 Discuss the use of a secure payment system with your bank. Verified by Visa and MasterCard SecureCode are recommended additional measures to secure payment systems
2 Ensure cardholder data is secure by complying with the Payment Card Industry Data Security Standard (PCI DSS)
3 Remain mindful that payment authorisation does NOT guarantee payment
4 Call customers to verify large online transaction details
5 Be wary of delivery addresses which are PO Boxes or those that are different from the billing address or telephone orders
6 Proceed with care when processing priority shipments for popular products among fraudsters such as TVs or mobile phones
7 Exercise caution when dealing with transactions from abroad
8 Be alert to changes in a customer's usual buying habits
9 Watch out for customers who use multiple cards to make purchases
10 Consider using a secure courier delivery service for high value products

Additional information can be found at **www.actionfraud.org.uk**

[10] All figures are from research carried out by Fellowes for National Identity Fraud Prevention Week 2010

5.3 **IDENTITY VERIFICATION**

Passports, driving licences, state or local authority benefit documents, current council tax bills or statements, current bank or credit card statements and utility bills can be used as a means of verifying a person's identity.

However, utility bills are not 100% reliable as a way of verifying identity, since they can be easily forged with a simple printer and scanner, so it is important to keep this in mind when using this document as a means of identity verification.

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

Paper security features

- Use ultraviolet (UV) light to detect fraudulent documents
- Look out for the quality of watermarks to verify documents
- Look for added fibres in the document, either visible to the naked eye, or under UV light

Printing security features

- Solid colours are used in genuine documents whereas fakes are often made using a series of dots using only three or four colours
- Optically variable inks are often used in genuine documents
- Microprinting is a feature that cannot be replicated using a traditional copier and scanner
- Fluorescent features are much more detailed in genuine documents

Other security features

- Uneven or absent perforations are a sign of a fake document
- Misspelling is a sign that documents are false
- It is easy to spot when bank stamps are fakes

Signatures

- There are two main components to a signature, 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 of which this subsection represents only a brief overview. When in any doubt, professional help should always be sought.

5.4 **CREDIT CHECKS**

A further essential weapon in the business' armoury against identity fraud is checking credit reports. Businesses are advised to do this for all employees and customers. Here are just some of the routes that companies can go down to verify an individual's or company's identity.

- Many agencies have services available to check the credit of an individual or business.
- Request a reference from the bank
- Request trade references from referees selected by you
- Request information from Companies House
- Check with the Insolvency Service. This maintains two facilities which provide information to the public, the Register of Individual Voluntary Arrangements (IVA) and the Bankruptcy Public Search Room (BPSR).

5.5 **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
- 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, ensuring that any changes made have been registered with the company's authority
- PROOF is supported by Companies House Web Filing Service and Software Filing services
- Companies House Web Filing Service is an online registration service for the secure submission of company information
- Both services require passwords, confidential authentication codes, and recognised email addresses

Further information at http://www.companieshouse.gov.uk/infoAndGuide/proof.shtml

5.6 **INFORMATION DESTRUCTION**

Backing-Up Business and Customer Data

In the running of their day-to-day business, all companies naturally have to keep hold of certain confidential information on employees, customers and suppliers. It is good practice to conduct regular risk assessments regarding the security of this data.

Companies should:

- Encrypt backed-up information that is held offsite (including whilst in transit)
- Carry out regular audits of encryption levels to ensure they match the current risk environment
- Back-up any data being transferred by secure internet links
- Ensure due diligence on third parties handling backed-up information to remain confident that it is secure, 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 so in accordance with accepted security policies and procedures
- Ensure that the company has 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 disposed of. Failure to do so could result in a data breach, for which the fine can be up to £500,000.

Companies should:

- Treat all paper generated as 'confidential' when no longer needed and ensure it is disposed of securely, for example by using cross-cut or microshred shredders – companies should never throw any documentation away without destroying it first
- 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 all electronic files to be deleted as soon as they are redundant and that files transferred to portable devices be wiped 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 companies use a third party supplier to destroy electronic equipment or corporate uniforms, make sure they have BSIA Accreditation
- Ensure that all members of staff are aware of, and sign up to your security policies
- Operate a zero tolerance policy with staff that flout company policy and/or compromise the safety and security of data

5.7 ONLINE SECURITY – HOW TO PROTECT YOUR BUSINESS FROM E-CRIME

E-crime is among the most prevalent of fraudulent activities with the effects often devastating Small and Medium Enterprises (SMEs). Awareness of the risks, combined with advice on measures to afford some protection are the first steps in combating exposure to e-crime and fraud.

Below is a series of simple precautions that must be put in place to ensure security:

Install anti-virus software, a firewall and anti-spyware on all IT systems

Install on every computer within the network environment a comprehensive security solution that includes anti-virus, anti-spam, firewall, spyware and malware (malicious software includes viruses, Trojans and worms), detection, removal, logging, quarantining and automatic updating.

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

Use a password at least eight characters long and a combination of different cases, numbers and characters
Introduce a password policy, to which users of the network must adhere.

Use caution when opening all emails and attachments
Ensure email security scanners are correctly configured, operational and up-to-date on the email hosting server and workstations opening the email. The scanner should target viruses, spam, Trojans, worms, malware and malicious content and phishing attacks.

Introduce an 'acceptable use' policy for internet and email
To remove any misunderstanding and clarify internet and email usage an 'acceptable use' policy should be developed to inform network users what behaviour is permitted by the company when using computing and network resources.

Keep up-to-date with patches and software updates
Download and install any operating system and application security updates and patches regularly as prescribed by the vendor.

Secure your wireless network
Change the default wireless access point (WAP) password. Disable automatic IP address allocation. Reduce the strength of the WAP signal if possible. Avoid WEP (wired equivalent privacy) encryption as this is considered a weak wireless encryption protocol.

Inform your clients of your data policy
Share your policy with your customers to ensure they do their part in protecting themselves and your company. Tell them you will never request their personal information by email or phone.

Encrypt your data and control who has access to it
Sensitive or confidential data should be encrypted or password protected and should not be transmitting over public networks which are unsafe, such as the internet or email, unless it is encrypted. This also applies to any confidential or sensitive data transferred onto an external storage device or media.

Backup data to guard against data loss
Create a back-up policy and clarify what data this applies to. Keep the backup systems offsite in a secure location in case of fire at the main site. Ensure on-site media is kept in a fireproof safe. If possible, use an online backup service.

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

5.8 CHECKLIST: HOW TO PROTECT YOUR ORGANISATION FROM CORPORATE IDENTITIY FRAUD

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, 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
- Store confidential or sensitive information in a secure place and limit access to key employees only
- Check your business' 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, email and 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 such as the business information agencies
- Put business bank account details and directors' signatures into the public domain (e.g. on your website or send to anyone via unencrypted email)
- 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
- 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, and therefore impersonate, one of your staff
- Throw away an old computer or laptop without wiping the hard-drive clean using specialist software first
- Leave documents in meeting rooms or on top of printers

5. WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

Additionally, different sectors have different regulations about what constitutes sensitive information:

Banking
- Loan applications
- Credit card statements
- Financial statements
- Mortgage applications
- Customer details
- Employee records
- Interest details
- Credit rating information

Education
- Pupil records
- Teacher information
- School reports
- Memos
- School letterheads
- Out-of-date chequebooks

Healthcare
- Patient details
- Employee records
- Blank prescriptions
- Letterheads
- Memos
- Prescription books

Public Sector
- Councillor and employee details
- Audit reports
- Council tax & housing benefit claims
- Memos
- Signed documents
- Finance plans
- Funding approvals
- Grant applications

For more information including checklists and support material, visit www.stop-idfraud.co.uk

6. THE IMPORTANCE OF REPORTING

SECTION 6 OBJECTIVES:

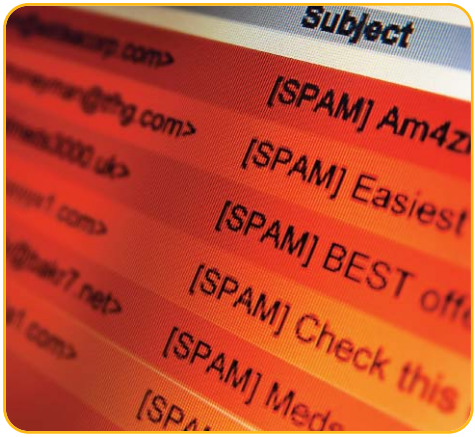
- **Examine the importance of reporting identity fraud**
- **Details of Action Fraud**

Although around 5% of small businesses are affected by fraud every year[11], 33% of small businesses that had experienced identity fraud do not report it. The prevailing attitude is that doing so would not accomplish anything. However, a significant minority (7%) indicated that they were not sure how to report it or who to contact.

In addition, many do not report viruses or phishing emails because they are seen as very common and therefore unworthy of bringing to the attention of the relevant authorities. It is only when fraud starts to affect the business coffers that it starts to be seen as fraud.

Businesses' reluctance to report identity fraud crimes helps criminals. There are many different institutions that can help track down and punish fraudsters, but they can only do so if businesses do their part and report breaches. When crimes are left unreported, criminals survive to attack other organisations and individuals and become more sophisticated in their approach.

Action Fraud, the UK's first fraud report and support centre, was recently launched to support businesses that have been victims of identity fraud. Crimes can be reported via the website www.actionfraud.org.uk or by phone on 0300 123 2040. Additional support tools can be found on the website.



[11] Research conducted by the Federation of Small Businesses

7. WHAT TO DO IF YOUR BUSINESS BECOMES A VICTIM

SECTION 7 OBJECTIVE:

- **Identify what steps to take to take if your business is affected by identity fraud**

Corporate identity fraud can have a financial and reputational impact on your organisation. Rectifying the damage caused by the fraudster, particularly to your credit rating, can take time.

SIX STEPS YOU SHOULD TAKE:

1. Report the matter to Action Fraud in the first instance. Contact the police if immediate police intervention is required. Notify Companies House and relevant suppliers
2. Inform your customers if their details may have been compromised or if 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
4. Keep a record of all correspondence you make or receive regarding the corporate identity fraud
5. Reassess your organisation's risk management and control systems to ensure that your business is adequately protected
6. Develop or revisit your data policy to ensure you remain protected

8. WHAT CAN YOU DO TO PROTECT YOUR OWN IDENTITY?

SECTION 8 OBJECTIVE:

- **Provide tips to help you 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 which areas of your life it applies. Below are some tips for individuals to consider, many of which apply equally well to your employees.

- Shred sensitive documents, such as financial statements, before throwing them away, preferably with a cross-cut shredder. Delete your name, address and account number from catalogues and direct mail offers too – or shred those pages as well.
- Never share passwords or PINs and don't write them down. Don't use the same PINs and passwords for multiple accounts.
- Redirect your post for at least six months after you move house. Give your new address to any organisations who regularly contact you.
- Ask the Post Office to investigate if important mail does not arrive. If you suspect your mail is being stolen or whether a mail redirection application has been made in your name without your knowledge, contact Royal Mail Customer Care on 08457 740 740. If you have a shared letterbox or communal hallway where post could be taken, ask for secure, individual facilities.
- Keep hackers and viruses out of your computer. Install the latest security software on your computer and update these programs regularly. Only use secure websites for online shopping – look for the closed padlock symbol or https:// at the start of the address.
- Never reply to emails asking for information such as account numbers, passwords and PINs. Don't click through to any website they direct you to. Check with the organisation the email appears to come from, using an existing number or email address, the phone book or a directory enquiries service. Never use the number given on the email.
- Don't give personal information to cold callers. This applies to the phone, the internet and face-to-face.
- Limit the information you share on social networks. Be especially careful of giving details such as dates of birth or children's names that you may use as PINs or passwords.
- Check your credit report regularly. If you see anything you don't recognise, contact the relevant lender immediately.
- Go through your bank, card and other statements carefully. Look for unfamiliar transactions that could indicate identity fraud.
- Pay attention to billing cycles - contact creditors immediately if your bills arrive late. A missing bill could mean a fraudster

WHAT CAN YOU DO TO PROTECT YOUR OWN IDENTITY?

has taken over your credit card account and changed your billing address.

- Investigate unexpected credit refusals. Your credit rating could have been ruined by a criminal borrowing money in your name and running up debts.
- Always tell the police and any organisations that might be affected if you suffer a theft of potentially sensitive items. For example, let your card issuer know if you've lost a credit card.
- Emailing or texting banking details – even to a trusted source – with unencrypted technology is a disaster waiting to happen.

These steps may seem simple, but they are important and effective yet, unfortunately, are 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 you and your family, visit **www.stop-idfraud.co.uk**

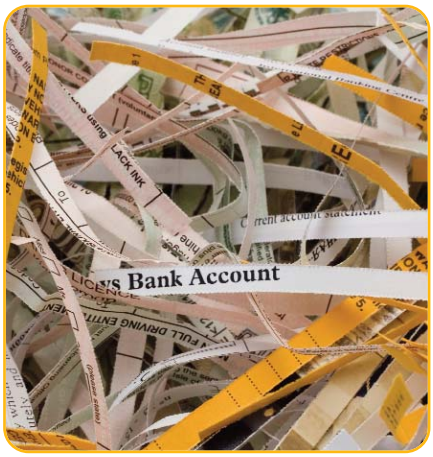
CASE STUDY: Lyndsey Briggs

Lyndsey Briggs is a married photographer in her 30s who suffered from current address fraud when a fraudster gained access to her private details.

After a holiday away last Christmas, Lyndsey received numerous letters for credit card applications and bank accounts opened in her name. Unsure of how anyone could have accessed her details she spent a considerable amount of time and energy trying to contact each of the banks and companies concerned, including Tesco, Natwest and MNBA. Fortunately no money was ever stolen, however, the fraudulent applications continue, most recently as June 2010.

"It really was a very scary experience. I have read about it happening to other people and how complicated it is to clear your name. I was worried it would be difficult trying to convince the banks that I was not the one making all the applications."

Lyndsey has since taken up ProtectMyID (PMID), a new comprehensive online service from Experian to allow consumers to keep track of where their personal information is being used to secure credit. She is relieved that as a PMID customer, a caseworker has taken care of everything and will contact all companies involved should anything similar happen again.



"Taking out CIFAS Protective Registration has been such a relief and my PMID caseworker was very prompt and helped to allay all my fears. It really was stressful calling each company to prove that it wasn't actually me opening the accounts, but thankfully I managed to take hold of the situation before it got out of control. I am now much more aware of who I give my details to!"

9. AFTERWORD

Dr Bernard Herdan
CEO
National Fraud Authority

"The theft of an identity underpins most serious crime. A stolen identity can be used to obtain money, property and goods as well as fund organised crime such as drug trafficking and terrorism. The consequences of ID theft can be devastating to both individuals and businesses. The financial loss suffered can cause bankruptcy and, in the case of businesses, can lead to closure.

The National Fraud Authority works closely with the counter-fraud community and industry to coordinate the effort to tackle this route into serious fraud. Much work has been and continues to be done to change practices and introduce barriers to ID fraud.

One of the key milestones we have achieved over the past year is the national rollout of Action Fraud, the UK's first national fraud reporting centre that provides a single point of contact for fraud victims where they can both report a fraud and seek guidance and advice. Businesses and individuals are able to seek advice, report crime and receive further support through Action Fraud. If you visit www.actionfraud.org.uk there are downloadable advice cards which can help businesses protect themselves against ID and other types of fraud.

I encourage businesses to follow the advice in this booklet and seek further advice from places like Action Fraud and www.stop-idfraud.co.uk. Preventing ID fraud can be quite straightforward and not at all costly. Raising staff awareness, regularly changing passwords and introducing document handling policies can sometimes be all it takes to make a critical difference to your businesses' safety."

10. ABOUT THIS GUIDE

Mind Your Own Business - A step-by-step guide to help protect you and your business from identity fraud was produced by Fellowes (www.fellowes.com) on behalf of and in conjunction with the associate organisers of National Identity Fraud Prevention Week 2010. 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:

- Simon Fitzgerald, Programme and New Developments Manager, CIFAS (www.cifas.org.uk)
- ACC Peter Lowton, ACPO Lead on Identity Crime and The National Identity Scheme, ACPO (www.acpo.police.uk)
- James Blake, Head of UK Identity Authentification, Experian (www.experian.co.uk)
- Kevin Burt, Identity Crime Policy Officer, Home Office (http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/index.htm)
- Neil Munroe, External Affairs Director, Equifax (http://www.equifax.co.uk)

National Identity Fraud Prevention Week 2010 is supported by Fellowes, the Metropolitan Police, the City of London Police, the National Fraud Authority, the Federation of Small Businesses, Equifax, CIFAS - The UK's Fraud Prevention Service, Call Credit, Experian, the Association of Chief Police Officers, the Home Office, the British Chambers of Commerce, the British Retail Consortium and the Royal Mail.

11. USEFUL CONTACTS AND RESOURCES

Further information

www.stop-idfraud.co.uk is a fraud prevention website 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 website has been launched as part of National Identity Fraud Prevention Week which is supported by:

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

11. USEFUL CONTACTS AND RESOURCES

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

- CIFAS – the UK's Fraud Prevention Service: www.cifas.org.uk
- Companies House: www.companieshouse.gov.uk
- Fraud Advisory Panel: www.fraudadvisorypanel.org
- Home Office Identity Fraud Communication Awareness Group: www.identitytheft.org.uk
- Metropolitan Police Operation Sterling: www.met.police.uk/fraudalert
- The Federation of Small Businesses: www.fsb.org.uk
- www.getsafeonline.org
- www.banksafeonline.org
- www.cardwatch.org.uk
- www.becardsmart.org.uk
- www.identitytheft.org.uk
- www.bcrc-uk.org (Business Crime Reduction Centre)
- www.fraudadvisorypanel.org
- www.keepyour.co.uk / (Nominet domain name advertising campaign)
- www.attorneygeneral.gov.uk/nfa
- www.financialfraudaction.org.uk
- www.experian.co.uk

Local Fraud Forums

- www.londonfraudforum.co.uk
- 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

NATIONAL IDENTITY FRAUD PREVENTION WEEK™

For more information on how to protect yourself, your business and your customers against identity fraud visit

www.stop-idfraud.co.uk

Supported by:

Fellowes · City of London Police · CIFAS · National Fraud Authority · British Chambers of Commerce · Metropolitan Police (Working together for a safer London) · FSB Federation of Small Businesses (The UK's Leading Business Organisation) · Royal Mail · British Retail Consortium (for successful and responsible retailing) · Equifax · Experian (A world of insight) · Callcredit (Part of the Callcredit Information Group) · Home Office