Fraud Advisory Panel

Identity Fraud: Do you know the signs?

A Practical Guide for Business

Disclaimer

Dissemination of the contents of this Guide is encouraged. Please give full acknowledgement of the source when reproducing extracts in other works.

Material is contained in this publication for which publishing permission has been sought, and for which copyright is acknowledged. Permission to reproduce material cannot be granted by the publishers and permission must be made to the copyright holder.

Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against you and/or your business and/or PC systems.

The Fraud Advisory Panel and the contributors to this Guide accept no responsibility for any action taken by parties as a result of reading this Guide. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them and/or their business.

Fraud Advisory Panel

fraud advisory panel

Identity Fraud: Do you know the signs?

A Practical Guide for Business

Acknowledgements

The Fraud Advisory Panel would like to thank Samantha Whitlock (ASB Law), Stephen Bassett (Wyse Leasing (Holdings) Ltd), and Mia Campbell (Fraud Advisory Panel), together with other members of the Cybercrime Working Group for their assistance in the preparation of this publication. Special thanks also to the original authors of *Identity Theft: Do you know the signs?*[1] on which this Guide is based.

[1] Fraud Advisory Panel (2003) *Identity Theft: Do you know the signs?* London.

Introduction

Identity fraud is a growing problem which is estimated to cost the United Kingdom (UK) economy £1.7 billion per year.[2] Individuals, sole traders, businesses and government departments can all become the victims of identity fraud.

- Over 4 million people in the UK claim to have been the victim of identity fraud at some stage.[3]
- In 2006 the number of identity frauds detected by members of CIFAS – the UK's Fraud Prevention Service (CIFAS) increased by 21.57% to 80,377 (up from 66,117 in 2005). The number of victims of impersonation also increased by almost 20%.[4]
- Corporate identity fraud is estimated to cost in excess of £50 million a year.[5]

The Fraud Advisory Panel has produced this Guide to help businesses manage the risk of identity fraud. The Guide covers the ways in which identity fraud can manifest itself, how to detect identity fraud and some of the steps that businesses can take to reduce the risk of becoming a victim.

The Fraud Advisory Panel is a registered charity comprising of volunteers drawn from the public and private sectors. Its role is to raise awareness of the immense social and economic damage caused by fraud and to help the public and private sectors, and the public at large, to fight back.

Corporate identity fraud occurs when a false corporate identity or another company's identity details are used to support unlawful activity.

This can include using a false corporate identity or another company's identity details for commercial, economic or monetary gain; or obtaining goods or information; or obtaining access to facilities or services.

Source: Home Office, Identity Fraud Steering Committee, www.identitytheft.org.uk.

[2] Home Office (2006) 'Identity fraud puts £1.7bn hole in Britain's pocket' press release, 2 February.

[3] Sainsbury's Bank (2006) 'Sainsbury's Bank offers identity theft protection' press release, 11 December.

[4] CIFAS – the UK's Fraud Prevention Service (2007) '2006 – fraud trends' press release, 30 January.

[5] Metropolitan Police Service (2005) 'Sterling work against corporate identity fraud' press release, 11 May.

What is identity fraud?

The term 'identity fraud' is commonly used to describe the increasingly prevalent fraud of impersonating another person or organisation for financial gain.

The methods used by fraudsters to obtain a business's identity information can vary considerably ranging from the simple (going through the rubbish or accessing information held by Companies House) to the more complex (hacking into the computer network or planting insiders within the business). This is often called corporate identity theft.

Fraudsters are now also targeting social and business networking websites such as Linkedin, Facebook and Myspace to obtain information on potential victims. This trend is likely to continue with the increasing popularity of these sites.[6]

One recent survey found that most data breaches that could facilitate identity theft were avoidable. Over 80% of all breaches were the theft or loss of a computer or other device capable of storing data or due to insecure security policies.[7]

The information obtained by fraudsters through these methods can then be used to purchase goods and services on credit, deceive customers, or take out loans – all in the business's name. This is identity fraud.

Businesses can be vulnerable to corporate identity fraud perpetrated internally by an employee, externally by individuals or organised criminals, or in collusion.

Types of identity fraud

Some of the common types of corporate identity fraud include:

- **Company hijacking** A fraudster submits false documents to Companies House to change the registered office address of a legitimate company and/or appoint 'rogue' directors without the knowledge or consent of the board of directors. The fraudster can then purchase goods and services on credit, sometimes through a reactivated dormant supplier account and then disappear before paying leaving the supplier out-of-pocket. It is estimated that approximately 50 false documents are filed with Companies House each month.[8]

[6] Rawstorne, T (2007) 'Facebook stole my identity' *Daily Mail*, 28 July, 56-57. Also see Palmer, M (2007) 'Fraudsters target social networkers' *Financial Times*, 22 August.

[7] Symantec (2007) *Symantec Internet Security Threat Report: Trends for July – December 06*.

[8] Digita (2006) *Keeping the Record Straight: Combatting Company Filing Fraud*. Also see Digita (2006) 'Company ID theft can be beaten' press release, 23 October.

- **Company impersonation** A fraudster impersonates a legitimate business, such as a bank, to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them. A business may be impersonated using phishing emails, bogus websites and false invoices. In some cases information on customers and/or suppliers is stolen or purchased in order to commit the fraud.
- **Long firm fraud** A fraudster sets up a new business (or in some cases purchases an existing one) which trades legitimately over a period of time and establishes a good credit history. Large orders are then placed and the fraudster disappears with the goods before paying, leaving the supplier out-of-pocket.

Preventing identity fraud

Corporate identity fraud should be treated as a business risk. Fraud, including corporate identity fraud, is a threat to the financial well-being of any organisation, its image and reputation.

Prevention is better than cure. There are a number of simple precautions that you can take to help safeguard your organisation's information and reduce the chances of becoming a victim of corporate identity fraud:

- Shred or destroy all documents containing confidential or sensitive business information *before* disposing of them. This may include company letterhead and compliment slips, customer details, bank statements and other financial information.
- Adopt a formal fraud policy statement and communicate it to all employees, contractors and suppliers. This should cover the organisation's response to theft, the acceptance and giving of gifts, unauthorised business expenditure and the use of assets. Undertake regular risk assessments and review your policy.
- Redirect your mail if your business moves premises and notify relevant organisations and customers of your new address and contact details.
- Screen all prospective employees *before* appointment and then on a regular basis. This should include temporary, part-time and contract employees – many scams still require an insider. Undertake additional checks on employees with access to personal and/or confidential information. CIFAS and the Chartered Institute of Personnel and Development (CIPD) have jointly produced guidance on how to prevent staff fraud (www.cifas.org.uk and www.cipd.co.uk)

- Check your business's registered details with Companies House on a regular basis to ensure that they have not been changed. This should include the address of your registered office and current director appointments.
- Consider registering for the protected online filing (PROOF) and monitoring services offered by Companies House (www.companieshouse.gov.uk).
- Invest in staff awareness and training. Include fraud prevention and detection within your induction programme and ongoing training. Educate all employees on how to recognise the risks of identity fraud and to ask questions.
- Check all customers *before* providing goods and services on credit. Request references from credible sources such as banks and credit reference agencies. Do not rely on information obtained from Companies House – it is a public record registry and does not verify the information it receives.
- Review your credit report on a regular basis for any accounts or credit applications in your organisation's name that you have not applied for. A fee is charged for these services.
- Introduce a clear desk policy and provide all employees with a lockable drawer and/or cabinet. Keep important documents and laptop computers secure.
- Implement clear reporting and whistle-blowing procedures for when fraud is detected against the business and/or your customers.
- Consider protecting your website by registering variations of your business's name (eg..com and.co.uk).[9] This may help reduce the threat of phishing attacks on your customers and the establishment of 'rogue' websites.
- Introduce an IT security policy that covers the internet, mobile devices, laptop computers, faxes, email and access rights and review it on a regular basis. Make all employees use secure passwords and screen savers. Encrypt information on wireless networks. Ensure old computers are destroyed and disposed of. Both the Department for Business, Enterprise and Regulatory Reform (www.berr.gov.uk) and Get Safe Online (www.getsafeonline.org) have produced information security advice for business.
- Introduce adequate internal controls to protect your business against fraudulent credit or debit card transactions, particularly card not present transactions. Advice for retailers is available from Card Watch (www.cardwatch.org.uk).

[9] Royal & SunAlliance (2006) 'Corporate identity theft to cost businesses £700 million a year' press release, 18 September.

The Fraud Advisory Panel has produced guidance for small- and medium-sized businesses (SMEs) on fighting fraud and protecting your IT systems which are available to download free from www.fraudadvisorypanel.org.

A checklist is available at the end of this Guide.

Obtaining your business's credit report

In the UK there are several credit reference agencies that hold information about businesses such as payment history, existing credit obligations, legal filings and background history. A copy of your organisation's (or another's) credit report can be obtained from these agencies for a fee. Credit references agencies include:

- **Dun & Bradstreet** (www.dnb.co.uk)
- **Equifax** (www.equifax.co.uk)
- **Experian** (www.experian.co.uk)

What to do if your business becomes a victim

There are a number of warning signs that may indicate that your business has become a victim of corporate identity fraud.

Has your business:

- Received letters or telephone calls from existing or prospective customers about 'official' correspondence purportedly from your organisation but which you did not send or make?
- Received letters or telephone calls from suppliers or other organisations about goods and services your business has not purchased or for lines of credit it has not opened?
- Had unauthorised changes made to its records at Companies House? This may include the address of your registered office and current director appointments.
- Been refused credit by suppliers when you thought it had a good credit history?

If you have answered 'yes' to any of these questions it may indicate that your business has become the victim of identity fraud. Do not ignore the problem – it will not go away and may get worse. Corporate identity fraud can adversely affect your organisation's credit rating and reputation.

T ake immediate action!

A lert your bank and/or credit card company immediately if your business's credit or bank accounts have been compromised.

K eep a record of all correspondence relating to the fraud.

E valuate your risk management processes and anti-fraud policies and make changes where necessary and appropriate.

A cquire a copy of your business's credit report and check it for discrepancies.

C onsider seeking legal advice from a specialist solicitor or Citizens Advice Bureau.

T ell the police where appropriate. [See **Reporting Fraud** section of this Guide].

I nform your customers if their details may have been compromised or a fraudster may have contacted them as a 'representative' of the business.

O btain a copy of your business's records at Companies House and check it for discrepancies.

N otify Royal Mail if you think your business mail is being tampered with.

Reporting fraud

Since 1 April 2007 a new process for reporting plastic card fraud has been introduced for individual merchants in England, Wales and Northern Ireland.

Individual merchants who are reimbursed by their financial institution should report plastic card fraud directly to that financial institution, not to the police. A report should only need to be made to the police by an individual merchant where he or she bears the loss.

Source: APACS (2007), Card Watch, www.cardwatch.org.uk

Legal recourse

There are three legal options available to your business if it becomes a victim of identity fraud. These are:

1. **Criminal prosecution** The Identity Cards Act 2006[10] and Fraud Act 2006[11] create new criminal offences for false representation and possessing documents for use in identity fraud. This includes possessing documents to be used for identity fraud, making a false representation on a website, and misusing a credit card to pay for a service.

   Your business must refer any alleged instances of identity fraud to the police in order for the fraudster to be prosecuted under the criminal law. Some larger organisations with in-house investigation teams 'package' their cases before referring them to the police.

2. **Civil recovery** Civil proceedings can present an alternative to a criminal prosecution and have the added advantage that your business may be able to recover some of its stolen assets.

   If your business does intend to recover losses caused by identity fraud through civil recovery it must be mindful of speed, surprise and strategy. At the very earliest opportunity you should assess:

   - whether there has been any fraud;
   - the extent of the fraud; and
   - whether it is viable to try and recover the losses sustained.

   In certain circumstances the English courts will assist victims of fraud by granting Orders which enable the victim, without notice to the fraudster, to discover:

   - the extent of the fraud;
   - who is responsible; and
   - who was involved in the commission of the fraud and therefore could be liable as well.

[10] Identity Cards Act 2006. Also see Explanatory Notes to Identity Cards Act 2006. Available from www.opsi.gov.uk.

[11] Fraud Act 2006. Also see Explanatory Notes to Fraud Act 2006. Available from www.opsi.gov.uk.

These may include third-party disclosure orders (where other parties have unknowingly been involved in the fraud), 'John Doe' orders (where the fraudster can only be identified by his acts not his name), and freezing and search orders. Third-party disclosure orders can also be combined with 'gagging' orders to prevent the third party notifying the fraudster.

Once the extent of the fraud has been assessed, a decision will need to be taken as to whether it is commercially sensible, or an obligation exists, to pursue the fraudster. Victims should also consider the significance of any adverse publicity which may accompany a decision to pursue a fraudster through civil proceedings.

3. **Parallel proceedings** A combination of criminal and civil proceedings.

Companies House

Companies House has a three point plan to assist registered businesses to prevent identity fraud. These are:

- **WebFiling** Businesses can file certain forms online with Companies House using an electronic password. The service is free.
- **Protected Online Filing** (PROOF) Businesses can file certain forms electronically with Companies House. Paper forms are rejected. The service is free.
- **Monitor** Businesses are alerted by email of any changes to their company details at Companies House. A fee is applicable.

Source: Companies House, www.companieshouse.gov.uk.

Protecting your business: a 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 including references, qualifications, experience and past employment.
- ✓ Securely destroy all documents containing confidential or sensitive business information before disposing of them.
- ✓ Store confidential or sensitive information in a secure place and limit access to key employees.
- ✓ 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 issues can be discussed without recrimination.
- ✓ 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 access. Review it on a regular basis.

Do not:

- ✗ 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 website).

Useful links

All Party Parliamentary Group on Identity Fraud
www.idfraud.org.uk

APACS – the UK Payment Association
www.apacs.org.uk

Bank Safe Online
www.banksafeonline.org.uk

Card Watch
www.cardwatch.org.uk

CIFAS – the UK's Fraud Prevention Service
www.cifas.org.uk

Citizens Advice Bureau
www.citizensadvice.org.uk

Companies House
www.companieshouse.gov.uk

Crimestoppers
www.crimestoppers-uk.org

Financial Services Authority
www.fsa.gov.uk

Get Safe Online
www.getsafeonline.org

Home Office Identity Fraud Steering Committee
www.identitytheft.org.uk

Law Society of England and Wales
www.lawsociety.org.uk

Law Society of Scotland
www.lawscot.org.uk

Metropolitan Police Service Fraud Alert
www.met.police.uk/fraudalert

National Identity Fraud Prevention Week
www.stop-idfraud.co.uk

Royal Mail
www.royalmail.com

For more information on the Fraud Advisory Panel please contact:

Fraud Advisory Panel
Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ

Tel: 020 7920 8721
Fax: 020 7920 8545
Email: info@fraudadvisorypanel.org

Or visit:
www.fraudadvisorypanel.org

Registered Charity No. 1108863

December 2007

OTHPLN6966 12/07