Fraud Advisory Panel

Identity Fraud: Do you know the signs?

A Practical Guide for Individuals

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 Individuals

Acknowledgements

The Fraud Advisory Panel would like to thank Samantha Whitlock (ASB Law), and Mia Campbell (Fraud Advisory Panel), together with 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 individuals 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 individuals 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.

Individual identity fraud occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud.

This can include using a false identity or someone else's identity details (e.g. name, current or previous address, date of birth etc) for commercial, economic or monetary gain; or obtaining goods or information; or obtaining access to facilities or services (such as opening a bank account, applying for a benefit or obtaining a loan/credit card).

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 person's identity information can vary considerably ranging from the simple (stealing your wallet or going through your rubbish) to the more complex (hacking into your computer or using hidden devices fitted at cash machines to obtain your debit card details). This is often called 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]

The information obtained by fraudsters through these methods can then be used to acquire new debit or credit cards, open bank or mobile phone accounts, obtain new passports or driving licences, apply for benefits, or take out loans – all in the person's name. This is identity fraud.

In a small number of cases the fraudster is known by the victim and may be a friend or family member.[7]

Types of identity fraud

Some common types of identity fraud include:

- **Application fraud and account takeovers** A fraudster applies for a new credit card or opens a new bank account in another person's name using pieces of personal and financial information that he or she has acquired. In some cases a fraudster may simply change a postal address of a legitimate bank customer to his or her own address.
- **Present (current) address fraud** A fraudster uses the name of another person living at the same address or nearby to purchase goods and services. The fraudster then intercepts the mail when it arrives. Present address fraud, which requires mail interception or redirection, currently accounts for almost half of all cases reported.[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] CIFAS – the UK's Fraud Prevention Service (2006) *Identity Fraud – What About the Victim?* Available from www.cifas.org.uk [Accessed 17 May 2007].

[8] Experian (2007) 'Experian sees rise in ID fraud coincide with increase in organised cyber crime' press release, 12 April. Also see CIFAS – the UK's Fraud Prevention Service (2007) 'Fraud trends cause concern' press release, 24 April.

- **Phishing** A fraudster sends emails to a large number of people claiming to be from a bank or other legitimate online business such as a shop or auction website. The email will usually contain a link to a fake but credible-looking website where the person is asked to update his or her personal information such as passwords and account details. The fraudster then uses this information to access the person's accounts.

Preventing identity fraud

Prevention is always better than cure. Treat your personal and financial information as an asset. There are a number of simple precautions that you can take to help safeguard your personal information and reduce the chances of becoming a victim of identity fraud:

- Shred or destroy all documents containing your personal information *before* disposing of them. This may include bank statements, utility bills, invoices, expired debit and credit cards and junk mail.
- Stop junk mail. Contact the Mailing Preference Service (MPS) to remove your name from mailing lists (www.mpsonline.org.uk). The MPS is a free service.
- Redirect your mail if you move house and notify relevant organisations of your new address. This may include utility companies, banks and mail order companies.
- Do not disclose personal information over the telephone, on the internet, by mail, or in person until you are able to confirm that the person is who he or she say he or she is. Be cautious about the amount of personal information you disclose on social networking websites.
- Review your bank and credit card statements on a regular basis for any transactions that you did not make. Keep your bank account details safe and consider closing any accounts that you no longer need.
- Make a note of your billing and bank statement cycles. Contact the relevant organisation if they are overdue.
- Review your credit report on a regular basis for any accounts or credit applications in your name that you have not applied for. Consider subscribing to one of the early warning services offered by credit reference agencies. A fee is charged for these services.
- Do not carry personal documents on you that you do not need. Leave them in a secure place at home. This may include your national insurance card, paying-in or cheque book, passport and birth certificate.

- Report any lost or stolen personal documents immediately. This may include your passport, driving licence, store loyalty card, and credit or debit card.
- Never let your credit or debit cards out of your sight in restaurants and shops. Shield the display when entering your PIN into a cash machine or mobile terminal.
- Ensure your home computer is adequately protected. Install anti-virus software and firewalls and keep them up to date. Make sure your wireless network is secure.
- Beware of phishing scams. Do not respond to any unsolicited emails you receive. Do not click on website links embedded in an email. Type the website address into the browser yourself, or access the website through a bookmark you have created.
- Make passwords secure by using a combination of numbers and letters. Do not disclose your passwords to others, and do not use the same password for different accounts.
- Consider carefully what information you store on mobile devices. Mobile devices such as phones, personal digital assistants (PDAs) and hand-held computers are more susceptible to loss or theft.

A checklist is available at the end of this Guide.

Obtaining your credit report

In the UK there are several credit reference agencies that hold information about individuals from a variety of sources including the electoral roll, County Court Judgments and lenders. This information is used by lenders to make decisions on whether to approve credit. A copy of your credit report can be obtained from these agencies for a small fee.

- **Callcredit** (www.callcredit.co.uk)
- **Equifax** (www.equifax.co.uk)
- **Experian** (www.experian.co.uk)

What to do if you become a victim

Reporting fraud

Since 1 April 2007 victims of credit or debit card, cheque and online banking fraud should report the matter directly to their bank or building society, not to the police.

It is the responsibility of the bank or building society to refer these types of frauds to the police in England, Wales and Northern Ireland. This change is designed to make it easier for victims to report these types of crime.

Source: APACS (2007) 'New Rules for Reporting Card, Cheque and Online Banking Fraud' press release, 30 March.

Many people do not realise that they have become a victim of identity fraud until contacted by a third party, such as a telephone company or electricity supplier.[9] However, there are a number of warning signs that may indicate that you have become a victim of identity fraud.

Have you:

- Started to receive mail for people who do not live at your address? Have you stopped receiving mail?
- Received letters or telephone calls from debt collectors or other organisations about goods and services that you did not purchase?
- Noticed unusual transactions on your bank and credit card statements that you did not make?
- Been declined a loan, mortgage and other financial product when you thought you had a good credit history?

If you have answered 'yes' to any of these questions it may indicate that you have become the victim of identity fraud. Do not ignore the problem – it will not go away and may get worse. Identity fraud can adversely affect your credit rating and may make it difficult for you to obtain credit in future.

In many cases you will not be liable for most of the debt incurred by a fraudster in your name. However, you will need to rectify the damage caused by the fraudster and this takes time. It has been estimated that the average amount of time this takes is between 3 – 48 hours.[10]

[9] Experian (2007) 'Experian sees rise in ID fraud coincide with increase in organised cyber crime' press release, 12 April; Also see CIFAS – the UK's Fraud Prevention Service (2006) *Identity Fraud – What About the Victim?* Available from www.cifas.org.uk [Accessed 17 May 2007].

[10] CIFAS – the UK's Fraud Prevention Service (2006) *Identity Fraud – What About the Victim?* Available from www.cifas.org.uk [Accessed 17 May 2007].

T ake immediate action!

A lert your bank and/or building society if you are the victim of fraud involving a credit or debit card, a cheque or online banking.

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

E valuate your current personal security strategies and make changes where necessary and appropriate.

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

C ontact any organisation that the fraudster has purchased goods and services from in your name.

T ell the police where necessary. Some organisations may require you to do this before they can investigate.[11]

I nvestigate the possibility of registering for protective registration through CIFAS. A small fee is charged for this service.[12]

O btain legal advice from a specialist solicitor or Citizens Advice Bureau if necessary.

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

[11] For cases involving a credit or debit card, a cheque or online banking your bank and/or building society should be able to advise you whether a separate report needs to be made to the police.

[12] CIFAS – the UK's Fraud Prevention Service, *Protective Registration Service*. Available from www.cifas.org.uk [Accessed 28 November 2007].

Legal recourse

In many cases it will be at the discretion of the business which supplied the goods and services to the fraudster to decide whether to prosecute (rather than the individual whose identity was used).

There are three legal options available to them. These are:

1. **Criminal prosecution** The Identity Cards Act 2006[13] and Fraud Act 2006[14] create new criminal offences for false representation and possessing documents for use in identity fraud.
2. **Civil recovery** Redress may also be sought through the civil courts to recover stolen assets. Civil proceedings can present an alternative to a criminal prosecution and have the added advantage that the victim may be able to recover some of his or her losses.
3. **Parallel proceedings** A combination of both criminal and civil proceedings.

10 point guide to protecting your identity online

1. Keep your wits about you at all times
2. Question why a website is asking for information about you
3. Never give any online security details to anyone unless it is completely necessary
4. Look after your password
5. Never click on links in emails
6. Keep (your software) up to date
7. Remove the spies (spyware)
8. Keep your connection secure
9. If it seems too good to be true, it probably is
10. Know where to go for help should you be a victim of online identity theft [see **Useful links** section of this Guide]

Source: BT plc (2006) *Security Report Online Identity Theft* www.btplc.com.

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

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

Protecting yourself: a checklist

Do:

- ✓ Securely destroy all documents containing personal information before disposing of them.
- ✓ Remove your name from unnecessary or unwanted mailing lists.
- ✓ Arrange for your mail to be redirected if you move house and notify relevant organisations.
- ✓ If you don't receive any mail check with Royal Mail that a redirection hasn't been set up in your name.
- ✓ Monitor your bank accounts regularly for any unusual transactions and close any bank accounts you no longer need.
- ✓ Review your credit report on a regular basis.
- ✓ Report lost or stolen personal documents and/or credit/debit cards.
- ✓ Limit the number of personal documents you carry to those that you need – leave the rest at home in a secure place.
- ✓ Use secure passwords and PINs – a combination of numbers and letters is best.
- ✓ Shield the display when entering your PIN into a cash machine or mobile terminal.
- ✓ Install anti-virus software and firewalls on your computer and keep them up to date.
- ✓ Limit the amount of information stored on mobile devices such as phones, PDAs and hand-held computers.

Do not:

- ✗ Disclose personal information over the telephone (especially a mobile phone), on the internet, by mail or in person to people you don't know.
- ✗ Respond to unsolicited emails.
- ✗ Disclose your passwords and PINs to other people.
- ✗ Use obvious passwords or PINs or the same password for different accounts.
- ✗ Let your debit or credit card out of your sight in restaurants and shops.
- ✗ Disclose personal information on websites that are not secure.

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

CardWatch
www.cardwatch.org.uk

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

Citizens Advice Bureau
www.citizensadvice.org.uk

Crimestoppers
www.crimestoppers-uk.org

Driver and Vehicle Licensing Agency
www.dvla.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

Mailing Preference Service
www.mpsonline.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

Telephone Preference Service
www.tpsonline.org.uk

Identity and Passport Service
www.ips.gov.uk

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

OTHPLN6967 12/07