

Identity Fraud

The term 'identity fraud' is commonly used to describe the impersonation of another person for financial gain. Fraudsters steal your personal identity and/or financial information and use it to purchase goods and services or to access facilities in your name.

What is identity fraud?

According to the Home Office Identity Fraud Steering Committee 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'.

Common types of identity fraud

Application fraud/account takeover:

A fraudster applies for financial services (eg, a new credit card or opens a new bank account) in your name or changes your postal address.

Impersonation of the deceased:

A fraudster uses the identity of a deceased person to obtain goods and/or services.

Phishing: A fraudster sends you an email claiming to be from your bank or other legitimate online business (eg, a shop or auction website) asking you to confirm or update your personal information such as passwords and account details via a link in the email.

Present (current) address fraud: A fraudster living at your address (eg, the same block of flats) or nearby uses your name to purchase goods and/or services and intercepts the mail when it arrives.

How does the fraud work?

A fraudster steals or acquires information about you. This may include:

- Your current or previous address
- Your date of birth
- Your bank account or credit/debit card details
- Any other personal or financial information about you

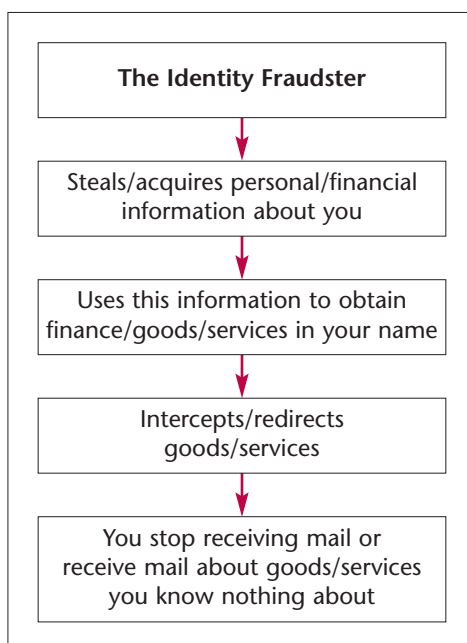
This information is then used to:

- Acquire new debit, credit or store cards
- Open bank or mobile phone accounts
- Obtain new passports or driving licences
- Apply for benefits
- Take out loans

All in your name.

You may not realise that you have been a victim of identity fraud for some time.

This is because the fraudster may intercept deliveries or redirect your mail without your knowledge or consent.



What happens if you become a victim?

Generally you will not be liable for all of the debt incurred by the fraudster in your name. However you will need to rectify the damage caused by the fraudster (particularly to your credit rating) and this can take time.

5 steps that you should take:

1. Report the matter to the relevant organisation(s) immediately. Follow their advice.
2. Obtain a copy of your credit report (available from credit reference agencies) and check for discrepancies. Go back to step 1.
3. Keep a record of all correspondence you make or receive in respect of the identity fraud.
4. Consider 'protective registration' through CIFAS – the UK's Fraud Prevention Service. A small annual fee is charged for this service.
5. Reassess your personal security strategies in respect of your personal and financial information. (Ask yourself 'how well do I protect it and can I do anything differently?')

In most cases it will be at the discretion of the organisation which supplied the goods and services to the fraudster to decide whether or not to prosecute. This is because the organisation supplying the goods or services is considered the victim in law – not you.

Reporting identity fraud

Credit or debit card, cheque and online banking fraud: Contact your financial institution. You do not need to make a separate report to the police unless instructed to do so (England, Wales and Northern Ireland only).

Other goods and services purchased in your name: Contact the relevant organisation. You may be asked to make a separate report to the police.

Loss or theft of passport: Contact the Identity and Passport Service.

Loss or theft of driving licences: Contact the Driver and Vehicle Licensing Authority (DVLA).

Loss or theft of mail: Contact Royal Mail.

Further information

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

Fraud Advisory Panel
www.fraudadvisorypanel.org

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

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.
Registered Charity No. 1108863

Disclaimer

Dissemination of the contents of this Fraud Fact Sheet is encouraged. Please give full acknowledgement of the source when reproducing extracts in other works. While every effort has been made in the preparation of this Fraud Fact Sheet, compliance with it does not guarantee that you will not be a victim of fraud or criminality aimed against you. The Fraud Advisory Panel and the contributors of this Fraud Fact Sheet accept no responsibility for any action taken by parties as a result of any view expressed herein. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them.

© Fraud Advisory Panel, 2008

How to protect yourself

Be aware of the risk from identity fraud and safeguard your personal and financial information.

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 without your knowledge.
- ✓ Monitor your bank accounts regularly for any unusual transactions and close any banks 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, even to family members.
- ✗ 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.

The Fraud Advisory Panel gratefully acknowledges the contribution of CIFAS – the UK's Fraud Prevention Service, Samantha Whitlock (ASB Law) and Mia Campbell (Fraud Advisory Panel) in the preparation of this Fraud Fact Sheet.

Distributed by the London Fraud Forum

