Protecting Your Identity

A PRACTICAL GUIDE

Contents

Introduction

When we think of crime we usually think of a physical action or violation against a person or a thing such as burglary, mugging or pick pocketing. However, in the twenty first century crime is taking a far more sophisticated form. One of the fastest growing crimes is identity fraud and it can be perpetrated without the criminals even breaking into your home. In a recent survey from credit reference agency Equifax a quarter of respondents claimed they had been victims of ID theft and over two thirds were concerned that they may be at risk. The last official estimate put the cost of identity theft at £1.3 billion, according to a Cabinet Office survey.

This practical guide explains what identity fraud is, how your identity can be stolen (identity theft) and the different types of identity fraud that can be committed using your name. It also offers you some simple steps to protect yourself from becoming a victim and a guide to what to do if your personal information is used fraudulently.

What Are Identity Theft And Identity Fraud?

Identity theft occurs when an individual's or company's personal or confidential information is obtained by another person without their knowledge in order to create a new false identity. Identity theft is the first step to perpetrating a criminal activity whereby criminals may use personal information to fraudulently obtain credit, goods or other services; this is known as identity fraud. Identity fraud can involve setting up a bank account in someone else's name, applying for a credit card or stealing a person's personality wholesale in order to fraudulently obtain goods, services, or other financial advantage, such as benefits. It can even extend to securing a passport in their name.

Corporate identity fraud may include stealing the identity of a company and fraudulently trading under that name without the knowledge of the legitimate company.

Criminals use a mixture of tactics to acquire the information needed to steal another's identity. They range from the very crude such as taking personal information from a stolen purse or wallet through to the bizarre; going through rubbish and the highly sophisticated 'phishing' or stealing somebody's identity online (See below for more information).

Worryingly for the victims of identity theft, they often do not realise their identity has been stolen until it is too late and they start receiving demands for loan repayments or bills for goods they have not purchased. In worst case scenarios innocent people have even been arrested for a crime they did not commit. Luckily most victims of identity fraud will not suffer financially. However this can take a huge amount of time and effort to put right the damage caused. (See How to Detect ID Fraud and What To Do If You Become A Victim)

How Can Your Identity Be Stolen?

In recent years, there has been an explosion of ways to collect, store, share - even steal - personal information about you. Your information has become big business and can be invaluable to an identity fraudster. Your identity can be stolen in any of the following ways:

Bin Raiding:

Fraudsters pay people to go through the rubbish you throw out, looking for bank and credit card statements, pre-approved credit offers, and tax information. Everyday information that you may not think is important such as old utility bills, insurance documents, bank statements and even personal letters carry valuable personal information that can be gathered together to steal an identity and create a fraudulent persona. A survey by British credit reference agency Experian into what Britons deposit in their bins found that 40 per cent of bins contained a credit or debit card number that could be linked to an individual while 75 per cent contained the full name and address of a member of the household.

Impersonation of the Deceased:

Ruthless criminals have been known to use the identities of deceased people to carry out fraudulent activity. Fraudsters will note the age, date of birth and address of deceased people from advertisements and announcements relating to the death or the funeral. Alarmingly, CIFAS - The UK's Fraud Prevention Service, estimates that there were over 70,000 cases of impersonations involving the use of identities belonging to the deceased in 2004. 'Day of the Jackal' frauds, where the dead individual was aged 18 or under, represent up to approximately 5,000 of the total.

Internet Sites:

Anybody that uses the internet will regularly be asked to share personal information about themselves to gain access to websites and buy goods. Tech savvy fraudsters can combine the personal information you share on unsecured internet sites such as your mother's maiden name with other bits of valuable information they glean about you to obtain credit in your name.

Mail Forwarding:

By completing change-of-address forms to redirect your mail fraudsters can receive a wealth of information about you delivered direct to their doorstep.

Phishing:

This term describes identity theft via email. Fraudsters will send an email claiming to be from a bank, credit card company or other organisation with whom you might have a relationship, asking for urgent information. Typically the email will ask you to enter your account details on the company's website to protect against fraud or to avoid your account being deactivated. If you click on the link in the email you will be taken to a website which looks genuine but has in fact been created by fraudsters to trick you into revealing secret information.

Skimming:

This usually occurs when a shop assistant or waiter gets your information by 'skimming' or copying your credit card information when you make a purchase. They often then sell the information to professional criminal gangs. Like phishing, skimming can be used on its own to collect enough information on your credit card to use your card fraudulently without stealing your entire identity.

Theft Of Wallet Or Purse:

The average purse or wallet contains bank cards, credit cards and valuable identity documents including driving licences and membership cards. Victims realise very quickly that their wallet has been stolen but often do not realise the value of the information contained within it until it is too late.

Unsolicited Contact:

Phone calls claiming to be from banks asking you to update your personal information should be regarded with caution. Calling the switchboard of the company in question and asking to be put through to the person who called you will help ensure you are not playing into the hands of fraudsters. Similarly, fraudsters posing as market researchers may ask for personal information over the phone. Credible organisations will not mind you double checking their authenticity before providing such information.

Corporate Identity Theft

It is not just the individual at risk, but also companies. By accessing publicly available company records fraudsters will change names of company principals and registered addresses. They will then trade off the back of the real company's good name and obtain goods and services on credit from suppliers. This is not the only area of risk. Company bank details may be in the public arena in order to encourage customers to pay for goods directly into the company's bank account. Fraudsters will obtain signatures from the public records and attempt to attack these company bank accounts by purporting to be the signatory on the account.

What Can Be Done With Your Stolen Identity?

A fraudster may use your personal information to get a car loan, acquire a phone or mobile phone service, or another utility service, or open a bank account in your name. Such cases can be seriously damaging to your credit history, since you may not realise anything is wrong until you notice unfamiliar charges on your monthly bills or statements or worse still you receive demands for payment from a credit card or loan company.

Types of fraud that criminals can perpetrate using your name include:

- **Opening new credit card accounts using your name. When they use the credit cards and don't pay the bills, the non-payment will appear on your credit report.**
- **Opening a phone or mobile phone account in your name.**
- **Opening a bank account in your name and writing fraudulent cheques on the account.**
- **Counterfeiting cheques or debit cards, and draining your bank account.**
- **Buying cars with loans in your name.**
- **Writing to your credit card issuer and, pretending to be you, changing the address on the account. Statements get sent to the new address, so you don't realise there's a problem until you check your credit report.**

Preventing Identity Fraud

Research from credit reference agency Experian reveals that on average it takes over a year to find out you are a victim of identity fraud and up to 500 hours to correct the situation. In March 2005, a poll by Populus, carried out on behalf of Fellowes showed that 81 per cent of the British Public were concerned about becoming a victim of identity theft. By managing your personal information carefully, and with a full understanding of its importance, you can substantially reduce the likelihood of becoming a victim of identity fraud. The following tips show you how:

Avoid Auto Complete:

Software that offers to remember your personal details to save you time when you next fill out a form online should be avoided. While the software itself is not fraudulent it can make it easier for thieves to access personal information about you if they successfully access your PC.

Be Vigilant:

Beware of anybody who contacts you unexpectedly and asks for personal information or account details even if they claim to be from your bank or the police. Ask for their name and a contact number and then check with the organisation in question before calling back.

Check The URL:

When you are online check the web address of the site you are visiting is spelt correctly as it is possible to be redirected to a similar name fraudulently. Better still, add the website to your favourites folder so that there can be no mistake you are going to the correct home page each time you log on.

Check Your Credit Report:

It is a good idea to check your credit report regularly to ensure nothing has been illegally set up in your name. Regular monitoring of your credit report will alert you if someone has been using your identity to obtain credit, ensuring you can not only rectify your credit report as soon as possible but also stop the fraudster in their tracks. You can obtain a copy of your credit report from both Equifax and Experian. (See Useful Contacts). The credit reference agencies also offer subscription monitoring services, which will alert you to any changes to your credit report via email or SMS.

Guard Your Cards:

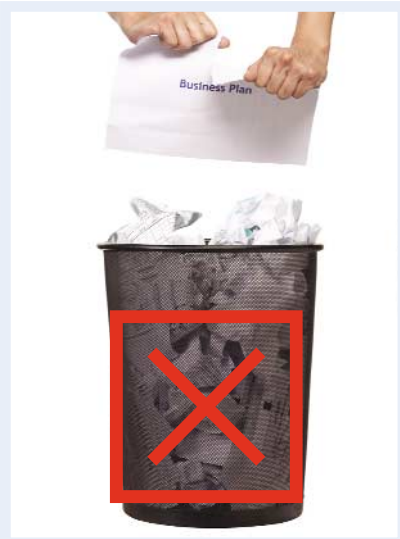
Minimise the information and the number of cards you carry in your wallet. If you lose a card, contact the fraud division of the credit card company. If you apply for a new credit card and it doesn't arrive in a reasonable time, contact the issuer. Watch cashiers when you give them your card for a purchase. When you receive a new card, sign it in permanent ink and activate it immediately.

Shred All Documents:

Shredding documents is the best way to ensure that criminals cannot build up a profile based on the information you discard in your rubbish. Invest in a robust shredder and make it a standard practise, whether at home or at work, to shred all documents containing personal or financial information before binning or recycling them. Cross cut shredders provide greater security by cutting paper into small confetti-like particles and also reduce bulk waste. Companies such as Fellowes offer affordable shredders for home and office use. (See Useful Contacts)

Passwords and PINs:

According to credit reference agency Equifax personal information such as your date of birth, address or mother's maiden name is enough information for a fraudster to open bank accounts, apply for credit cards, loans and much more. Memorise your passwords and personal identification numbers instead of carrying them with you. Avoid using easily available information like your mother's maiden name, your birth date, your phone number, or a series of consecutive numbers and don't use the same pin number for all your cards and accounts.



Pay Attention To Billing Cycles:

Contact creditors immediately if your bills arrive late. A missing bill could mean a fraudster has taken over your credit card account and changed your billing address.

Personal Information:

Whether on the phone, by mail, or on the Internet, never give anyone your credit card number or other personal information for a purpose you don't understand. Ask to use other types of identifiers when possible.

Protect Your Post:

Deposit outgoing post in post office collection boxes or at your local post office rather than leaving it in office out trays or similar. Promptly remove post from your post box after it's delivered. If you plan to go away, contact the Royal Mail about its Keepsafe service which helps you avoid that tell-tale pile of unopened mail on your doormat. Keepsafe will hold your mail for up to two months, and deliver it on your return. For more information see **www.postoffice.co.uk**

Stay Safe Online:

If you use the internet make sure you have the latest security patches and up-to-date anti-virus software installed.

Update Contact Details:

According to the latest research from Experian, nearly half of identity thefts are perpetrated at previous addresses. If you move house or change phone numbers tell all relevant organisations about the change as soon as possible. Using a mail forwarding service for at least six months is a good way to make sure all post is redirected to your new home and reducing the risk of your personal information getting into the wrong hands.

Useful Numbers:

Keep a record of the numbers you need to ring if your credit or debit cards are stolen. You have to cancel your cards as soon as possible after they have been stolen to make sure they cannot be misused.

Simple Steps for Businesses to Protect Themselves

Of course, it is not just individuals that can fall foul of identity thieves. Businesses too can be targeted by ruthless criminals. But, just like individuals, companies can put measures in place to make it harder for criminals to use their organisation for criminal activity. Many of the rules that apply to individuals can be adapted to protect companies. Other steps for businesses to consider include:

Check Identity:

Always check the identity of your customers, both businesses and consumers. Credit reference agencies offer a wide range of solutions to authenticate and verify the identity of customers to ensure that they exist and are who they say they are.

Companies House:

1. **Check your 'REGISTERED DETAILS' (Directors, Company Secretary and Company Address) at Companies House.** Make sure these are correct and that they have not been fraudulently changed.

2. **File your documents online and sign up for 'PROOF' at Companies House.** In January 2005 Companies House introduced 'PROOF', a free, password protected, online system for companies to alter their details on the register. This system is far more secure than the existing paper record system as no changes can be made without the password.

   For further details about PROOF, contact **0870 3333636** or visit **www.companieshouse.gov.uk.**

3. **Sign up to an 'alert' system that will warn you of any changes to your company details**. Companies House and all the major credit reference agencies have suitable subscription systems in place at nominal cost. These will promptly alert you if any changes are made to your company's details.

4. **Do not rely on Companies House records alone if determining whether to lend goods or service on credit.** Companies House is a public record and not a crime prevention service or credit reference agency. Always satisfy yourself that your customer is legitimate through additional means.

Company Bank Accounts:

Do not allow details of the main company account to be in the public domain where fraudsters may obtain sufficient detail to facilitate an attack on the account through impersonating the signatories.

Document Procedures:

Having a well formulated document disposal policy in place and adhering to it is the first crucial step in protecting your business and employees from identity fraud.

Store Sensitive Documents:

Lock away sensitive documents in a safe place and limit access to these documents to the staff who really need them. Fellowes has produced an R-Kive Record Management handbook detailing how companies can store sensitive information safely and offering useful tips and hints, including legal requirements relating to document retention.
(See Useful Contacts)

Shred All Documents:

Businesses have a duty of care to protect their customers' and employees' information and a legal obligation under the Data Protection Act to keep it up-to-date and accurate. Shredding documents is the best way to dispose of documents securely and to ensure that criminals cannot gain access to sensitive company information fraudulently.
Cross cut shredders provide greater security by cutting paper into small confetti-like particles and also reduce bulk waste. Companies such as Fellowes offer affordable shredders for home and office use. (See Useful Contacts).

Inform Staff:

Informing staff about the risks of corporate identity fraud will ensure they remain vigilant. Caution them about the risk of giving out company information online or over the phone without first checking to whom they are giving the information.

How To Spot Identity Fraud

The best way to spot identity fraud early is to stay vigilant. Monitor your accounts and credit agreements closely as nobody knows your financial habits or is better equipped to spot fraudulent activity better than you. The following are useful tips to help you spot fraud as soon as it happens:

Monitor Billing Cycles:

A missing bill or bank statement could mean someone has taken over your credit card account and changed your billing address. Keep a note of the date you expect bank statements and utility bills to arrive and contact the relevant parties if they are late.

Check Your Statements:

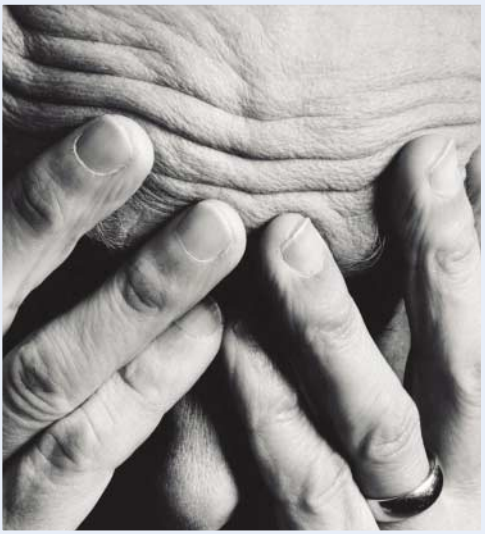
Review bank and credit card statements and keep an eye out for unusual transactions you do not immediately recognise. Do not be afraid to follow up with your bank or credit card company to see if they can provide more information about the transaction if you think it looks suspicious.

Monitor Your Credit Report:

Unless you check and monitor your credit report frequently with a company like Equifax or Experian to ensure they are up to date and accurate there is often no way to tell if identity thieves have used your personal information to open credit accounts or other services in your name.

What To Do If You Become A Victim

If you suspect that someone has used your name, or other personal information to get credit or a loan, the following steps can help.



Contact Your Bank And Credit Card Companies:

Contact your bank/building society and credit card provider to cancel any cards. Even if not all your accounts have been affected it is worth flagging the issue to other lenders, banks etc so they can monitor your accounts more closely and ensure that the thieves do not access these

Contact A Credit Checking Agency:

Contact a credit checking agency such as Experian or Equifax and follow their suggested steps to resolve the situation and prevent it happening again. (See Useful Contacts)

Protective Registration from CIFAS:

Contact CIFAS, the UK's Fraud Prevention Service, and file a Protective Registration notice on your credit file. This will flag to potential lenders that you have been a victim of identity fraud and greater security measures will be taken to ensure that the application for credit is genuine. (See Useful Contacts).

Freeze Fraudulent Accounts:

Contact the appropriate creditors, banks, phone companies, and utility companies and have them freeze the accounts. You may be liable for only £50 of the fraudulent charges, but different issuers have different policies. Most creditors promptly issue replacement cards with new account numbers.

Call The Police:

Report the crime to the police department that has jurisdiction in your case and request a police report. Though the authorities are often unable to help, a report may be necessary to help convince creditors that someone else has opened an account in your name.

Keep A Record:

Because recovering from identity theft can be a long and complicated process, it's important to keep a record of all communications. Send all letters by registered mail and keep copies. If you think your case might lead to a lawsuit, keep track of how much time you spend dealing with the problem.

Contact Crimestoppers:

Crimestoppers has been operating its **0800 555 111** phone number in the UK since 1988, allowing people to phone in anonymously with information about criminals or crimes which are then passed on to the police.

Useful Contacts

CIFAS
www.cifas.org.uk

Companies House
www.companieshouse.gov.uk

Crimestoppers
Crimestoppers allows people to phone in anonymously with information about criminals or crimes which is then passed on to the police.
Tel: 0800 555 111
www.crimestoppers-uk.org

Equifax
Tel: 0870 0100 583
www.equifax.co.uk

Experian
Tel: 0870 241 6212
www.experian.co.uk
www.creditexpert.co.uk

Federation of Small Businesses
Tel: 020 7592 8100
www.fsb.org.uk

Fellowes
Tel: freefone 00 800 1810 1810
www.fellowes.co.uk

Financial Services Authority
Tel: 020 7676 1000
www.fsa.gov.uk

Fraud Advisory Panel
Tel: 020 7920 8721
www.fraudadvisorypanel.org

Home Office
www.identity-theft.org.uk.

Inland Revenue
www.inlandrevenue.gov.uk

Metropolitan Police Fraud Squad
Tel: 020 7230 1256
www.met.police.uk/fraudalert

Royal Mail
Tel: 08457 740 740
www.royalmail.com


METROPOLITAN
POLICE
Working together for a safer London


FSB


Fellowes


experian®


EQUIFAX


CRIMESTOPPERS
0800 555 111
Call anonymously with information about crime


CIFAS

www.fellowes.co.uk