

LAWPACK



*Self-Help Kit*

# ID Theft Protection

Guidance Manual



This is an excerpt from Lawpack's *Identity Theft Kit*.

To find out more about how you can protect yourself from identity theft, [click here](#).

#### EXCLUSION OF LIABILITY AND DISCLAIMER

Whilst every effort has been made to ensure that this Lawpack Kit provides accurate and expert guidance, it is impossible to predict all the circumstances in which it may be used. Accordingly, neither the publisher, author, retailer, nor any other supplier shall be liable to any person or entity with respect to any loss or damage caused or alleged to be caused by the information contained in or omitted from this Lawpack Kit.

Lawpack gives you a limited guarantee. If for any reason you are not happy with your purchase, you may return it to us with your receipt within 30 days of the date of purchase for a full refund. In no event shall our liability exceed the purchase price of this Kit. Use of this Lawpack Kit constitutes acceptance of these terms.

This Lawpack Kit may not be reproduced in whole or in part in any form without written permission from the publisher, except that forms may be photocopied by the purchaser for his or her own use, but not for resale.

Figures quoted are correct as at 1 January 2008

# Contents

How to use this Kit	5
Introduction	7
<b>Examples of how identity theft can affect you</b>	9
Card-not-present fraud ('CNP')	9
Having your credit card 'skimmed'	9
Theft of your credit cards	10
Theft of your personal details by people at your last address	11
Stealing your bank details	12
Airport theft	14
Checking in at hotels	14
Advance fee scams ('419' scams)	15
Abuse of social network websites	16
Theft of your personal details from within a company	16
Buying expensive items on eBay	16
Theft of your personal details from someone close to you	17
Bin bag theft	17
Giving away your personal details inadvertently	18
Mortgage refinancing schemes	18
Fraudulent address change of your existing credit card	18
Targetting your old hard disk information	19
Fraudulent mail redirection	19
A job offer you cannot refuse	20
Car buying nightmare	21
Putting your personal details on a school or work reunion site	21
Goods order for your company, but not by you	22
You are a retailer and suffer unjustified chargebacks	23
<b>Initiatives to reduce the threat</b>	24
The law	24
Identity cards	26
Lost and stolen documents register	27
Electoral roll opt-out	27
Credit file monitoring	28
Password disciplines	35
Identity theft insurance	36
Increased card security	36
<b>Warning signs</b>	38
You are unexpectedly declined credit	38
Your credit card is refused unexpectedly	38

Your credit card company calls to query a foreign or unusual transaction	39
You find accounts you do not recognise on your credit file	39
The police arrive with a warrant for your arrest	39
Your cheques bounce unexpectedly	39
Mail appears to be late, or bunched, or fails to arrive	40
You are burgled, but nothing much seems to have been taken	40
A County Court summons arrives for a debt you know nothing about	40
A debt collector, bailiff or Sheriff's Officer arrives at your door	40
You receive a debt collection call at work for an unknown debt	40
You receive an overseas health claim on a Form E111 in your name	40
You receive notice from your local post office that a redirection notice requires renewal	41
You are stopped unexpectedly when you try to leave or enter an airport	41
<b>Prevention</b>	42
Essential	42
Financial fraud prevention	42
Recommended actions	43
Web disciplines	43
Travelling	44
If you are a director of a company	44
If you have purchased UK domain names in your personal name	44
If you move house	44
<b>Specimen letters</b>	45
<b>Loose-leaf</b>	
Victim Assistance Checklist	
Useful Contacts Checklist	

# Examples of how identity theft can affect you

Understanding some of the ways that identity theft can occur can help you to know when you are most at risk. After reading these examples, you will quickly learn to safeguard your basic personal information.

You may be shocked by how easy it is to impersonate someone else. In some cases it is so easy that, for security reasons, we have not revealed exactly how it is done.

Please look carefully at our tips to help you to reduce the chances of becoming a victim of identity theft. In many cases they involve no cost; just a small change to your habits.

## Card-not-present fraud ('CNP')

---

According to the UK trade association for payments, APACS, the only area of credit card fraud that continues to rise is internet, phone and mail order transactions – known as 'card-not-present' or 'CNP' fraud. These transactions account for the lion's share of fraud losses in 2006 at £183.2m, up 21 per cent from £183.2m in 2005.

To combat 'CNP' fraud losses, most cards now have a security number on the security strip on the reverse of the card, which is required to be quoted when using the card. This will mean that the simple theft of credit card number databases will no longer be as valuable to criminals, as without knowledge of the security code printed on the reverse of the card, some retailers will refuse to accept the card.

### TIPS

1. When you are buying online or by phone make sure that you provide your security number only to reputable companies.
2. Avoid companies who seek your card details on an order form that you have to post off to them. There is a risk that if your order is intercepted, your card could be skimmed (see below).
3. When buying online, look for the little yellow padlock on the bottom of the screen when you get to the payment page. Hover your mouse over it and check that the site is properly secured.

## Having your credit card 'skimmed'

---

This happens when your card details are stolen when you use your card in a perfectly normal manner. The employee who processes your transaction takes a copy of your

details, returns your card to you normally, and then sells the details to an organised crime ring.

The details are used either to purchase goods by telephone or internet (card-not-present transactions) or are used to construct a convincing but fake credit card containing your details which is then used in the usual way.

Fraud losses through 'skimming' amounted to £96.8m per annum in 2005, down 25 per cent, due principally to the introduction of 'chip and PIN' technology.

You are most at risk when you use your card in places with very high levels of card activity that are not local to you. Restaurants in major cities or resorts, or petrol stations, tend to be high-risk areas for 'skimming'.

Transactions by criminals using stolen card details or fake cards often occur in the Far East or in the US. Your card company monitors your card usage and will eventually spot a transaction which is not consistent with your normal behaviour, or which is physically impossible (e.g. if you appear to purchase goods near home within a hour of your fake card being used in Malaysia).

#### TIPS

1. Be wary of suspicious delays in obtaining authorisation. If you suspect abuse, do not challenge the assistant. Instead, notify your concerns to the fraud department of your card issuer straight away.
2. Check your credit card statements on receipt for any suspicious transactions and report it to your card issuer if you have any concerns.
3. Consider using a single card for petrol station and restaurant use. This helps you to spot unusual transactions on the card most at risk.
4. Always notify your card company before you travel abroad. Each card company has its own policy on this. Some need to know, whereas others will advise you that they do not.

## Theft of your credit cards

Fraud on lost and stolen cards is the second largest type of card fraud and amounts to £68.4m, down some 23 per cent from 2006, thanks largely to the introduction of 'chip and PIN'. Strictly speaking this is not classed as identity fraud – it is a simple case of theft.

Someone steals your purse or wallet, or better still – because you may not notice for a while – a single card from it and uses your card posing as you. You will know from experience that your signature is rarely challenged.

Until the card limit is reached, the criminal is unlikely to be detected, but even so will regard the first decline of an attempted transaction as a warning sign to change his or her spending habits. The card will continue to be used, even when it is 'over the limit', as the criminal will then spend smaller amounts beneath the 'floor limit' of shops. When card transactions are undertaken below the floor limit of each retail outlet, no automatic checks of the card are made with your card company. Fraudulent usage will continue, at a slower pace, and remains unlikely to be detected at the point of sale, as most thieves are cunning enough to know the floor limits and adjust their spending accordingly.

Eventually your card balance will be substantially in excess of your credit limit and the card company will usually telephone you, unless you have already spotted the unusual transactions when examining your monthly statement.

#### TIPS

1. Only carry as many cards as you actually need. Do you really need your gold card for supermarket shopping?
2. Keep cards you do not carry in a secure place and check regularly that these have not been stolen.
3. Cancel cards you do not use. If someone used a dormant card unlawfully, you probably would not notice for some time.
4. If you have high card limits that you never use, think about asking your card issuer to reduce your limit to a lower amount.
5. Look carefully at your signature. Is it really easy to forge? If so, consider making it harder to imitate.
6. Keep your cheque book separate from your cheque guarantee card.
7. These tips apply similarly to debit cards, which carry a slightly greater risk because your bank details, including account number and bank sort code, are often shown on the card.
8. When travelling in countries where the risk of theft is high, think about using travellers cheques and local currency instead of credit cards. The top ten credit card fraud hotspots, according to Barclaycard, are:
  - (i) Turkey
  - (ii) France
  - (iii) Spain
  - (iv) USA
  - (v) Italy
  - (vi) China
  - (vii) Thailand
  - (viii) Ireland
  - (ix) India
  - (x) The Netherlands

## Theft of your personal details by people at your last address

When moving house, many people fail to inform all companies of a change of address. Post may continue to be delivered to old addresses from insurance companies, pension companies and mobile phone companies. Similarly, junk mail, including pre-approved offers for credit, will continue to be received for a short while after you move.

Identity theft criminals can respond to such offers to obtain cards in your name and use the letters addressed to you for authentication purposes.

**TIPS**

1. Check your credit files regularly – see page 29 on how to do so. These will show all of your accounts still active at previous addresses, and any new accounts opened.
2. When you move home, put mail redirection in place for at least a year. When you receive redirected mail, make sure that you advise the sender of your new address.

## Stealing your banking details

---

If you use internet banking, beware of emails that appear to come from your bank. When they are fraudulent, the emails typically contain a link that when clicked will pass you to a convincing copy of the bank's website, which has been set up specifically to obtain customers' user names and passwords. It is very easy to copy the images and logos from the genuine website to a fake email, and equally easy to 'cloak' the sender's address in such a way as to make it appear that it comes from a bank.

Customers of Barclays, Citibank, Egg, Halifax, Lloyds TSB and NatWest have already been targeted by criminals in this way. Criminals prefer to fake the websites of larger financial institutions to increase the possibility of finding customers using junk email.

According to the National Criminal Intelligence Service (NCIS), most people cannot distinguish between the genuine bank website and a fraudulent copy, which makes it easy for organised criminals to target online banking customers in an attempt to gain access to their accounts. This type of identity theft is called 'phishing'.

Bear in mind that no one from any financial institution, or indeed from any reputable company, will ever ring you and ask you for your account number and password.

**TIPS**

1. Never click on an emailed link purporting to connect you to your bank and treat all emails from your bank as suspicious. Generally, banks do not email you.
2. If you can avoid the temptation, never click on any email link contained in any junk email. If you really must visit the site, type it in to the address bar on your browser to reduce the risk of abuse.
3. Keep control of your email addresses. Consider using several; one for your friends and family, one that is only disclosed to trusted sources and one for general use.
4. Study the examples opposite to help you spot similar phishing scams. Note the similarity between examples of phishing emails (a) and (b) which were distributed widely in October and November 2006. The 'From' address was cloaked to make it appear that the message originated from Barclays Bank Plc or from The Co-operative Bank Plc. This is very easy to do and fools many people.  
Barclays Bank has the dubious honour of being the first bank in the UK to be attacked by phishing scams such as this.

(a)

 **BARCLAYS** Online Banking:  
Barclays UK • Barclays International  
Personal Banking • Business Banking • Premier Banking


**Customer Details Confirmation Procedure**  
personal/business/premier banking

Dear Barclays customer,  
Barclays bank's technical services department is carrying out a scheduled software upgrade to improve the quality of services for the bank's customers.  
We urgently request you to go to the link below and confirm your bank details.  
<http://www.barclays.co.uk/brcontrol.taskstart.custbase/detailsconfirm>

These instructions are being sent to all Barclays bank customers.  
We apologise for the inconvenience and thank you for your co-operation.

**Barclays Bank PLC. 2006**

(b)

 **The COOPERATIVE BANK**  
Customer led, ethically guided

Dear **The Co-operative Bank client,**

The Co-operative Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.  
By clicking on the link below you will begin the procedure of the user details confirmation.

<http://www.co-operativebank.co.uk/satellite/userinfo/coopbank.asp>


These instructions are to be sent to and followed by all the Co-operative Bank clients.  
We apologize for any inconvenience and thank you for cooperation.


The Co-operative Bank Technical Service


The Co-operative Bank is authorised and regulated by the Financial Services Authority (No. 121885).  
The Co-operative Bank p.l.c., (990937) P.O. Box 101, 1 Balloon Street, Manchester, M60 4EP.


(c)

Cc:  
Subject: Natwest invites you to trial FastPay, the no nonsense online Payment service

You have received this email thanks to a Thomson Directories partner 



 SIGN UP NOW

 Sign up now  
for a free trial  
(offer ends 12th January)

**FastPay: the easy way to sell online.**

Dear Miss Phillip  
Thousands of people are making money selling online, offering everything from clothing to computers. The quick and simple way to join them is FastPay - the no nonsense online payment service. And what's more if you sign up by the 12th January 2004 you get a **Free Trial** until 1st March 2004.

FastPay benefits:

- FREE to set up
- higher account limits - up to £5,000
- accept payments on your website - with the FastPay payment button
- receive payments quickly and be informed the moment they arrive
- customers can use debit cards, credit cards or a bank account to fund payments.

The above, more sophisticated, email example, (c), was distributed in January 2004. Perhaps of more concern, initial enquiries of NatWest confirmed that the email was genuine, yet on careful examination the mail did not come from NatWest, but from an obscure Italian web address, and some of the links did not work. Criminals can hijack genuine emails, logos, text and graphics, and change the links and return addresses very easily. If you have the slightest doubt at all about any email, just delete it, as the risks of falling victim to a phishing scam are too high.

## Airport theft

Criminals target people at airports, as travellers tend to be easily distracted and usually have all their important identity documents, cards and money in one easy to identify place.

What is more, the simple act of removing or reading a luggage label can help thieves to identify properties likely to be vacant for the next seven to 14 days.

### TIPS

1. Keep your travel documents separate from your money and try to keep them on you, and not in your hand luggage.
2. Do not put your home address on blatant display on your luggage labels. Put your home address inside your case, and, if practical for the homeward part of your journey, use your work address instead, or simply quote your mobile phone number.

## Checking in at hotels

Similarly, checking in at hotels provides a wealth of information about you. Your home address, telephone number, the length of your absence from home and even your credit card details are often taken when checking in.

Most hotels are careful to keep records securely and dispose of them when they are no longer required, but dishonest staff can easily take copies that can become the basis for simple credit card theft.

### TIPS

1. Consider leaving a small cash deposit for 'incidentals' rather than a credit card impression. Alternatively, obtain a payment card, such as the Unique card ([www.theuniquecard.com](http://www.theuniquecard.com)), that can be topped up but used in a similar way to a credit card.
2. If it is practical, use your work address with your work telephone number, or your mobile number, instead of your home telephone number, when you register.

## Advance fee scams ('419 scams')

---

Emails seeking fees in advance are an international scam, although many which seek help to bring money specifically out of West Africa are fairly common.

Despite widespread publicity these emails continue to dupe people relentlessly and are called '419' scams. Section 419 of the Nigeria Criminal Code was specifically enacted to help prevent this type of fraud, and despite many high profile prosecutions, the sheer amount of money that can be gained by criminals is such that the scam remains extremely rife. In 2003, the Nigerian government established the Economic and Financial Crimes Commission (EFCC) to combat 419 scams, because the scale of losses are at a level that they are dissuading foreign investment into Nigeria generally.

A typical example starts as follows:

'...I am HAJIYA MARYAM ABACHA, wife of the late Nigeria Head of State, General Sanni Abacha, who died on the 8th of June 1998 while still on active duty. I am contacting you in view of the fact that we will be of great assistance to each other and can develop a cordial relationship....."

The email goes on to say that she has £45m from a Russian contract, which needs to be forwarded to a safe haven outside Nigeria and if you are able to provide your UK banking details, so that your account can be used to receive the monies, she will pay 20 per cent of the proceeds to you as a reward. Those who respond are leaving themselves likely to become a victim of identity theft after disclosing personal information, in particular their date and place of birth, address, credit card or bank account details.

A commonly held belief is that 419 scams tend to prey on individuals with little financial awareness and that the victims are driven solely by greed, but this is not so. Recent successful targets include companies, schools, churches and charities. The largest single prosecution by the EFCC to date – in 2003 – involved the duping of Brazilian bank manager Nelson Sakaguchi of the sum of US\$242 million.

### TIPS

1. Never respond to any suspicious emails. Any email seeking your co-operation to move cash is likely to be a scam. Just delete this type of email.
2. Never give your personal financial details to anyone by email. Email is not a secure method of communication, so reputable companies would never ask you to do this.
3. Be careful when giving your email address to anyone. If you receive a 419 scam, this means that the criminals already have your email address.
4. A light-hearted approach to advance fee scams can be found on [www.scambuster419.co.uk](http://www.scambuster419.co.uk), which includes details of how typical 419 scams progress if they are pursued.

## Abuse of social network websites

---

The growing popularity of social networking websites, such as myspace.com, has extended its audience beyond teenagers and young people to adults. Care needs to be exercised when adding any personal information to a profile that may be viewed by others and abused.

### TIPS

1. If you use social networking websites or even blogs, consider creating a profile using an alias.
2. Avoid publishing too much personal information and, in particular, your date of birth or place of birth on such sites.
3. Bear in mind that sometimes such sites are subject to US law, not UK law, so you may not be fully protected by the Data Protection Act 1998, as explained on page 24.

## Theft of your personal details from within a company

---

Although all companies are required by law to safeguard the security of your personal information, disgruntled employees can steal information relatively easily.

In the US, this was the method used by the criminal behind one of the largest ever identity theft crime attempts. Personal data of over 60,000 staff were offered for sale over the internet by a former tax department employee of the Prudential Insurance Company, as part of a credit card scam, but local police detected the crime and successfully prosecuted the criminal following an undercover operation.

There are regular, reported incidents of the inadvertent loss or theft of personal information from companies. In November 2006, the Nationwide Building Society revealed that a laptop had been stolen in August 2006, containing personal details of its 11m customers, but fortunately it did not contain customer passwords or memorable information.

### TIPS

1. If you believe that information given to one company has been used by another, ask the first company why they have disclosed your data. Your action in challenging the use of data may help alert a company to internal leakage of data.
2. If you see personal data being traded and you suspect that it is being sold unlawfully, report the matter to the police.

## Buying expensive items on eBay

---

An escrow account is a type held by the auction site so that the sale proceeds are only released when both sides are happy with their sides of the transaction. Criminals can

find simple ways of impersonating you to unlock your side of the escrow, which we are not about to reveal here, leaving you without the goods and without the money.

#### TIPS

1. For high value items, insist on payment in advance.
2. Make sure that any cheques are cleared before you release the goods.

## Theft of your personal details from someone close to you

---

Approximately half of identity theft issues in the UK are believed to be committed by persons who know their victims personally. This may be in the workplace, home or in a social environment.

#### TIPS

1. Be very careful with your cards, PIN numbers and personal identifiers, such as your place of birth and your mother's maiden name.
2. Do not use the same passwords or PIN numbers everywhere. This is a disaster waiting to happen.
3. Bear in mind that there is nothing worse than a scorned family member or co-worker. Keep your PIN to yourself.
4. After a relationship breakdown or change of employment, change your passwords and PIN numbers.

## Bin bag theft

---

For some time, debt collectors and investigators have stolen bin bags put out for collection. By carefully examining discarded rubbish, it is relatively easy to identify assets that can be seized by creditors.

Similarly, identity theft criminals sift through rubbish to find personal details and letters that can be used to help 'authenticate' a new identity. This practice is relatively rare but is often cited as being linked to the growth of identity theft crime. In the US the practice is known as 'dumpster diving'.

#### TIPS

1. Shred all confidential letters and statements before putting them in the bin. Use a cross-cut shredder in preference to a ribbon-cut shredder. But be conscious that no matter how good the shredder is, a determined thief can always reconstruct any document.
2. If you do not have a shredder, tear up the documents and separate the pieces into several bins, or burn them.

## Giving away your personal details inadvertently

---

Be wary of surveys or competitions that ask for contact details, or requests to be added to free directories, or which offer shopping vouchers in exchange for a survey of your lifestyle habits. Some of these are little more than a contrived method of seeking your basic personal details. In many cases the information gained will be sold to many companies.

### TIPS

1. If in doubt, do not respond.
2. Subscribe to the various opt-out services, such as the Mailing Preference Service, listed in the Useful Contacts Checklist. If you subscribe and still get approached, you will know the approach to you is suspicious.
3. Opt out of having your electoral roll details used for marketing purposes. See page 28 on how to do this.

## Mortgage refinancing schemes

---

Criminals pretending to be mortgage consultants or mortgage lenders may approach you to offer very tempting remortgage or equity release schemes. The email or letters may look very convincing, with genuine logos and marketing literature copied from a major mortgage lender, but the return address or phone number will be cleverly changed to that of the criminal.

Because mortgage applications require the most comprehensive information of all credit applications, and the law requires mortgage lenders to undertake a detailed 'fact find' to enable you to be given the best advice, this is an easy method for criminals to obtain your personal data for the basis of impersonation fraud.

### TIPS

1. In general, never respond to such offers. Instead, use an established high-street or well-known internet broker.
2. If you are in any way unsure, check that the broker has a Consumer Credit Licence by enquiring with the Office of Fair Trading by phone on 0845 722 4499 and also consider undertaking a company search using a business credit reference agency – see 'Checking Companies' in the Useful Contacts Checklist.

## Fraudulent address change of your existing credit card

---

The criminal calls your card issuer and advises of a change of address. A few weeks later, he or she reports your card missing. The replacement card is sent to the fraudulent address and the criminal uses your card without your knowledge.

**TIPS**

1. Card companies have methods of reducing this risk, which for obvious reasons are not detailed here, but these are not foolproof.
2. This method is only effective if the criminal already has your personal identifiers, such as your place of birth, mother's maiden name and password. Keep these safe.
3. Find out when your bank and credit card statements are due to be received each month and if you do not receive any on the due dates, ring the bank or card company and ask why.
4. Consider tracking the use of your card by using internet-based credit cards that allow you to view recent transactions and statements online.
5. Have your credit files checked regularly (see page 29). These will not only advise you of current balances and limits, but also of new accounts and any new addresses registered against your name.

## Targetting your old hard disk information

---

Never sell a desktop computer, word processor or laptop computer without first erasing data using proprietary software. Criminals scan newspapers for sellers of PCs and will pay good cash for an unerased hard drive.

**TIPS**

1. Use an eraser – at least three times – even though this may take many hours. Physical destruction of a hard drive is the only truly safe method of destroying the data contained on it.
2. When throwing away old floppy disks or recordable compact discs, make them unreadable first by physically damaging them.

## Fraudulent mail redirection

---

One of the simplest ways of finding out a great deal about you is to intercept your mail, using the Royal Mail's redirection service. Although procedures have been tightened to reduce the risk of mail interception, this remains a favourite of identity theft criminals.

Do not be fooled into thinking that you might notice total absence of mail. Experienced criminals will identify items of little or no interest to them and have these put into your post box, so that only a small proportion of your post is retained. If the criminal gets lucky, he or she might even intercept a new or replacement credit card or driving licence.

Most often, criminals use mail redirection when they apply for credit in your name. Your current address then becomes your previous address, and the fraud is committed from an address unconnected with you. Thieves can intercept any requests for further information and obtain the card (and even 'activate' it) entirely without your knowledge.

**TIPS**

1. Query with your local post office any suspiciously delayed mail.
2. If you are telephoned or approached by a lender about a credit application of which you have no knowledge, make it clear to them that this may be impersonation fraud and check with your local post office to see whether a redirection notice has been placed against your address.
3. Speak to your neighbours. Sometimes an identity theft attack is a concerted effort on several houses in the same street.
4. If you do not have mail delivered directly to your door (e.g. you may use a gate-mounted external post box or, if you live in a flat, the post may be spread on a desk in a communal hall), be more wary of the relative ease of intercepting your mail.

## A job offer you cannot refuse

---

You receive a call from a headhunter, or you see an advertisement for a particularly well-paid job with an established, reputable company. Eagerly, you send in your CV to the Human Resources (HR) Director.

A few days later you are phoned with the good news that you have been shortlisted for an interview and are, in fact, the favoured candidate. An interview will be arranged at genuine company offices within a few weeks. In the meantime, the caller advises you that you need to provide some additional information so that the employer can undertake some background checks to ensure compliance with the Financial Services Act, or with some other (plausible) European law. The information that will be sought will be your place of birth and mother's maiden name. The caller will also ask for your bank address so that a bank reference can be obtained.

You will turn up for the interview. The HR Director is indeed the right person, but is not aware of the vacancy. Finally, when you check your bank account you find it drained of all your funds.

**TIPS**

1. Never give your mother's maiden name or place of birth to anyone you do not trust. These items are not usually required by employers, so be suspicious of anyone that asks for them.
2. If the job seems too good to be true, it probably is.
3. Limit your CV to basic facts.
4. View any approach from a headhunter with some suspicion.
5. If you are in doubt, telephone the company concerned to speak directly with the interviewer before sending in your CV. Obtain the number from the telephone directory and not from any letter received, purporting to come from the company concerned.

## Car buying nightmare

---

A driving licence is stolen. A criminal uses this to purchase a car from a motor dealer in the name given on the licence, on hire purchase (HP), using the licence as identification. The finance company compares signatures on the HP agreement with the driving licence and they appear to match.

Credit checks made by the finance company prove satisfactory, so the finance company provides the money direct to the dealer (less a small cash deposit) and the criminal drives off with the car. He promptly sells the car to you, an innocent party, provides you with valid documentation and then disappears.

No payments are ever made on the loan, so the finance company contacts the driving licence holder, who has no knowledge of the transaction. The finance company checks the details of the current keeper with the Driver and Vehicle Licensing Agency (DVLA), and then repossesses the car – from you.

As the law stands (the Hire Purchase Act 1964) a person selling a car subject to HP cannot pass on a 'good title' (which means that in law, the person cannot sell) to the innocent buyer, so the car remains the property of the finance company. The law provides some protection for innocent buyers (under Section 27 of the same Act), but where the HP agreement has been forged, that protection does not apply, so you will lose the car, and your money with it.

### TIPS

1. Always obtain a car check – see 'Checking Vehicles' in the Useful Contacts Checklist – before purchasing a vehicle to ensure that no HP remains outstanding.
2. If your driving licence is stolen, consider having your credit file monitored so that any attempt to raise finance in your name is quickly identified.
3. Have your credit file monitored. Regular checks will ensure that if someone obtains car finance in your name, you will be alerted to it reasonably quickly.

## Putting your personal details on a school or work reunion site

---

You add your name to a website that helps old school friends to find each other. You decline to add a message for reasons of personal privacy. Because of the structure of the way that school lists are displayed on such sites by school year, a criminal can view your entry and calculate your year of birth.

As there is a fair chance that your school is near your place of birth, an identity thief can infer details and lawfully obtain purchase from the Registry of Births Marriages and Deaths a copy of your birth certificate. If abroad, the thief can even obtain it on the government's website for the General Register Office ([www.gro.gov.uk](http://www.gro.gov.uk)) for £10.

Armed with your birth certificate and after searching for your current address using easily accessible methods, such as a public telephone directory or an electoral roll website, a criminal has sufficient data (even your mother's maiden name) to cause real damage.

#### TIPS

1. Understand the risks involved of using such sites. The more responsible ones enable you to remove your details completely and easily.
2. If you are concerned, ask to be removed from websites such as [www.192.com](http://www.192.com) that sell the electoral roll – they will be pleased to do this free of charge if you do so by post using the form on their website.
3. Be aware that websites such as the above simply report information that is already in the public domain. The electoral roll is on public display in libraries, so removal of your name and address from them will not completely remove the risk of abuse from other public sources.

## Goods ordered for your company, but not by you

You receive a phone call from one of the large office supply multiples chasing payment for a considerable amount of goods purchased many weeks previously – supposedly in your name. Because of previous frauds, the office supply company tells you that before it sent the deliveries, it had checked that the delivery address matched the company's registered address. It soon becomes clear that the orders were made for the company but delivered to a different registered address than your own company.

After viewing Companies House documents, you find that someone has filed a Form 287 against your company to change the registered address for a brief period. Once the form had been accepted at Companies House, the criminal made the purchases from the office supply company and then filed another Form 287 at Companies House to change the address back.

This is a summary of a crime committed against Sky Marketing Limited in November 2003, where the office supply company involved was Staples. Using similar methods, an identity theft criminal could equally have changed the names of directors and have negotiated a bank loan, or have used stolen cheques to draw monies from your current account, with minimal risk of detection.

#### TIPS

1. If you are a director of a company, large or small, you can arrange for all changes at Companies House to be notified to you by a business credit reference agency – see 'Checking Companies' in the Useful Contacts Checklist – sometimes for free.
2. Make sure that the person handling your invoices is made aware of this risk, so that unusual invoices or demands are dealt with urgently.

## You are a retailer and suffer unjustified chargebacks

A chargeback is the reversal of a credit card transaction by a genuine cardholder, and is often the result of a cardholder checking his or her card statements and finding items that are not recognised.

For 'card-not-present' retailers, such as those dealing by mail order, telephone or over the internet, this is a major issue as under current card rules the loss must be borne by the retailer rather than the card issuer.

If a retailer suffers a higher than average level of chargebacks over several months, the merchant services provider (the intermediary that processes card payments) can fine the retailer a significant sum of money and ultimately can withdraw the retailer's ability to accept credit cards.

### TIPS

1. If you sell online, consider whether you need to make additional checks for those purchasers who have yahoo or hotmail email addresses. Research by the Credit Reporting Agency in 2006 revealed that a purchaser with a yahoo email address is seven times more likely to chargeback a transaction. Hotmail email addresses are similarly more loss-prone. In the UK, yahoo.co.uk addresses are untraceable and are the 'weapon of choice' for identity thieves.
2. For high value transactions, use the free National Chargeback Register on [www.creditreporting.co.uk](http://www.creditreporting.co.uk). This enables retailers and others to record details of all known chargebacks in real time, so that 'hot cards' can easily be identified before goods or services are released.