

Identity crisis

Article from Which? March 2005 (Copied with permission)

How to avoid becoming a victim of identity fraud, and what to do if the worst happens

Being burgled is a traumatic experience, but for Bob Armstrong it was just the beginning of his troubles. The burglars stole a briefcase, containing his wallet, cheque book, mobile phone and a couple of items of mail. This was the start of an elaborate identity scam which ended up costing £21,000. Bob took the obvious first step of cancelling his cards, but this wasn't enough to prevent the crime.

He believes the thieves found his date of birth on some mail and used public records to find out his birthplace and mother's maiden name. They then intercepted the new cards ordered by Bob, and activated them using this information. They wrote £21,000 worth of cheques from Bob's accounts and paid them into his credit card accounts, before taking them out again as cash.

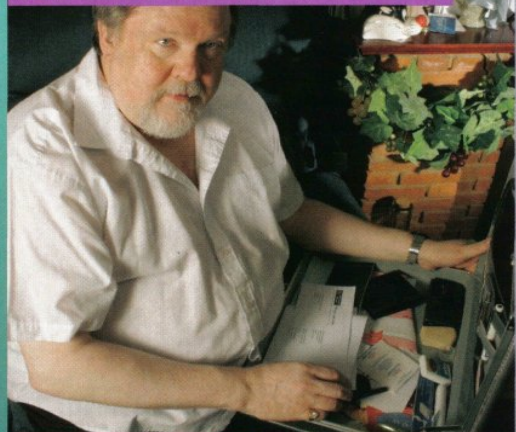
Bob was astonished at the temerity of the criminals. 'I couldn't believe how easy it was for them,' he told us. 'If they have your name and date of birth, anyone can trawl the internet to find everything they need. It is ludicrous that it is so easy to find this information.'

Bob had always checked his bank statements carefully but this crime took place in just ten days. It was left to the bank to inform him of the unusual transactions. He said: *'I'm now very careful not to keep all my documents in one place. The trauma isn't worth it.'*

WHAT IS ID FRAUD?

Bob's not alone. Identity fraud is one of the fastest-growing crimes in the UK - government estimates that it costs the country £1.3 billion a year. A quarter of UK adults know someone who has had their identity taken and misused, or have experienced it themselves, according to our latest survey. It's no wonder that more than two thirds of you told us you're concerned about ID fraud. Your identity is valuable to criminals for a variety of reasons. If someone can pass themselves off as you, they can gain access to your bank accounts and steal your money, or run up huge credit card bills. Equally, a stolen identity can be used to setup bank accounts for

“With your name and date of birth, anyone can trawl the internet to find all they need” Bob Armstrong



money laundering or benefit fraud; it can even be used for people trafficking. *'Identity theft can be a harrowing experience,'* says Peter Hurst, Chief Executive of fraud prevention service Cifas. *'It can be months before it's discovered, and sometimes takes just as long to sort out.'*

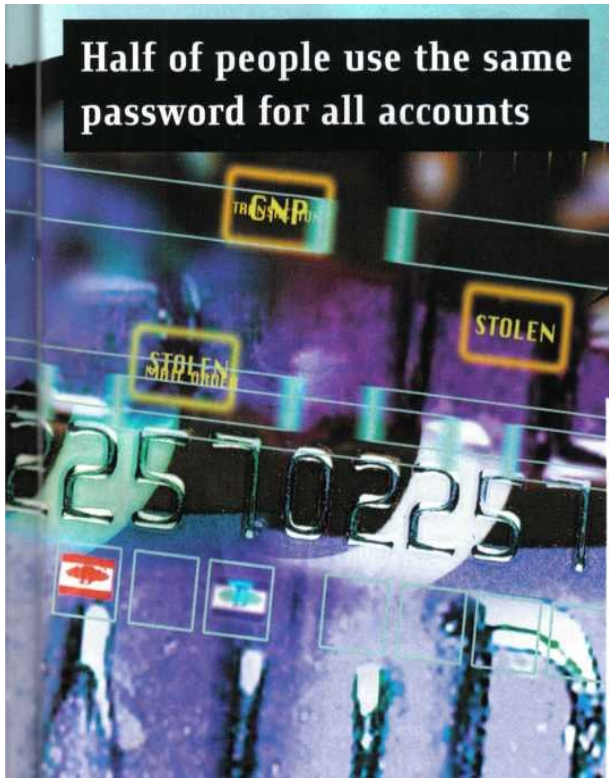
Because your identity is a valuable commodity, criminals have become ever more ingenious in their quest to get hold of a convincing false identity. While direct theft of valuable documents is one approach, criminals don't always have to mug you or burgle your house to use your details.

VIRTUAL FRAUD

New technology and the internet have opened up brand-new criminal industries. Spam emails often contain viruses that can be used by hackers to access sensitive information on your PC. Alternatively, 'phishing' emails are sent. These are designed to look like correspondence from a bank, and typically ask you to reply confirming your security details, or include a link to a fake bank web site. Some of these emails can look extremely professional - even containing your bank's logo - so you should always treat any unsolicited email with extreme caution.

Cold calling is a similar technique. *'You receive a phone call from your "bank", normally in the morning or early evening when you're probably busy,'* says Jill Stevens of credit reference agency Experian. *'They tell you that they suspect your card has been used fraudulently, so they're checking to see if you've made a certain transaction'.*

As part of the spiel you're taken through your security details to check you've got the card on you. 'Before you know it, you may have given your mother's maiden name, or your Pin,' says Jill. A genuine call or email from your bank should never ask you to give sensitive security details so don't ever hand them over unless you've contacted your bank yourself.



Half of people use the same password for all accounts

HOW YOU CAN PROTECT YOURSELF

ID fraud costs £1.3bn a year

Two thirds worry about ID fraud

With Ken's advice in mind, you might be forgiven for deciding to live in a cave without a phone, and paying for everything in cash that you've kept in a sock under the bed. Fortunately there are ways to protect yourself and lots of them are free:

Barry Stamp runs checkmyfile.com, a website that offers a range of ID fraud prevention services. He told us: 'There are easy steps you can take to reduce the risk of fraud. Don't carry documents around unless you need to - you don't need to carry your driving licence unless you're hiring a car. And don't ever carry your address in your wallet.'

Ken agrees: '*Lots of burglaries now happen with the sole purpose of stealing bank details or identity documents. If you can, keep them locked up. If not, don't keep them all together in an obvious place.*'

PROTECT YOUR PASSWORDS

Worryingly, half of you use the same password for all your accounts, according to our survey. Think carefully about any passwords you have on your bank accounts - don't use the same password for each one, especially if it's something obvious like your first-born's name. And never write passwords down or give the information out unless you're sure you're talking to someone legitimate.

Banks should never contact you cold and ask for your security details. If they do, you should refuse to give them and say you'll contact them through the normal channels, such as their customer services number.

REDIRECT YOUR MAIL

If you're moving house, you're particularly vulnerable to potential scammers, as our own car expert Dave Evans found out. Dave moved house recently, and redirected his post to his new address. He didn't notice anything was amiss until he bumped into his local postman, who told him that his redirected mail had been redirected once again, to a third address. Dave said: '*I was aghast at how easy it was to do. The Post Office requires two forms of ID, but the scammers managed to do it. I caught it before any money was lost, but it was lucky I knew my postie.*'

The fraudsters had also asked BT to reconnect Dave's phone line. This meant that they could get hold of an introductory letter to use as proof of address, which they used to apply for credit cards in Dave's name at the fake address. Dave redirected his post again just in time - as he soon started to receive the new cards he hadn't applied for.

While Dave's experience was extreme, you must make sure you contact every company which might send you mail if you change addresses. It's easy to forget items such as registered share certificates, or rarely used credit cards, during the hassle of a move.

'Even unsolicited mail can give away sensitive information,' says Jill Stevens, *'and this may*

continue to be sent to your old address after you move.' One solution to this problem is to register with the Mailing Preference Service (see www.mpsonline.org.uk) which can remove your name from 95 per cent of direct mailing lists. *'Redirecting your mail for at least a year and registering on the MPS is important,'* says Jill. *'Experian also advises people to check their credit reports two or three months after moving. It will highlight any applications in your name that you otherwise might not have been aware of.'*

CHECK BEFORE YOU CHUCK

Probably the easiest bit of advice is not to put anything sensitive in the bin. According to our survey, about half of the UK population now destroys utility bills or receipts, but we should all be doing it. *'Shred everything you don't need to keep -that's what I do,'* says Ken Farrow, and as a member of the Fraud Squad he's well placed to give advice.

Paper shredders can be picked up reasonably cheaply, but a more low-tech solution is to rip up any bank statements or bills before you bin them, making sure you deface any sensitive numbers or addresses.

WHAT TO DO IF YOUR ID IS STOLEN

If identity documents, such as your driving licence or passport, have been stolen, and you are concerned you may be a victim of ID fraud, you can pay £11.75 for the Protective Registration Service run by Cifas. Next time you apply for credit, it won't be approved automatically but instead will be referred for checks. This may include confirming your identity.

Peter Hurst of Cifas, told us: 'If you buy a TV on in-store credit (especially in the evenings or on Sunday), you may not be able to take it away that day. But most people don't mind this if it means they have peace of mind.'

It's worth paying £2 to each of the three credit reference agencies (Experian, Equifax and Callcredit) for a basic search of your credit file. All three offer more expensive services, such as reformatting your credit report to make it easier to read, but a basic search gives all the information you'll need.

If someone has used your identity to open an account or buy goods, immediately contact the company with which the fraudsters have taken

out credit. Speed is key. Neil Munroe, External Affairs Director of Equifax, told us: 'I would suggest that you make haste and urgently contact them by phone. Follow it up with a letter, so that you have it in writing. Then apply for your credit file and check for any unusual applications.'

Once you have reported the problem to the credit lenders, an automatic Victim of 'impersonation' marker will be added to your credit file. You won't be charged, but it will mean that any new credit you apply for won't be approved immediately.

At the same time, contact your local police station and get a crime reference number. Don't ignore the problem. It can affect your credit record and you may have difficulty obtaining credit in the future.

Peter Hurst of Cifas admits that, *'to start with, you may be regarded as the prime suspect, as it is very difficult for the companies to tell who is the perpetrator and who is the victim. There have even been cases of people pretending to be victims just to avoid paying their own debts.'*

The hassle entailed in clearing their names is often the biggest problem for victims. There was probably little that Bob Armstrong could have done to prevent his crime. He wasn't liable for the stolen cash but it took him months to sort out.

Peter Hurst agrees: *'I've seen cases where the fraudsters have opened 30 to 40 accounts in the name, and it can take up to a year to stop the correspondence from coming.'* Neil Munroe of Equifax told us: *'It can take up to 300 hours to fully clear your name.'*

The final straw for Bob Armstrong was when he contacted his credit card provider to activate his new cards. 'I changed my passwords and made sure I used something very random that only I would know. Yet, when I rang them, they asked me only for my mother's maiden name. I was incandescent with rage, especially after the efforts that I'd made to prevent this!'

WHAT IS BEING DONE

Spending days trying to prove that someone else isn't who they say they are isn't much fun. While there's a lot you can do to make it difficult for criminals, sometimes there's nothing you can do to prevent someone using your identity.

One problem you can't do much about is inside

jobs in financial institutions. Ken Farrow suggests that many banking fraud cases involve insiders: *'City of London Police is working closely with the banking industry, particularly with regards to the security of temporary staff. Many have excellent procedures in place, but they employ a lot of staff, and unless thorough vetting is carried out, there is always the possibility of a bad apple slipping into the organisation.'*

The Association of Payment Clearing Services (Apacs), the main industry body representing card issuers, says that fighting ID fraud is one of the industry's top priorities. *'The ongoing investment in fraud prevention from the banks is phenomenal and growing all the time. This money is going into training staff and co-ordinating databases to spot unusual applications,'* it told us.

We'd like to see banks being more vigilant about security. Mother's maiden name or place of birth should never be used as default passwords. We easily got hold of the editor's place of birth and mother's maiden name - see 'Stealing the ed's ID' opposite. Some banks do ask questions about your account activity, which is a start, although of course it breaks down if someone's got hold of your statement from the bin.

Apacs adds that the banks are improving their procedures: They are starting to put in place more stringent security checks for high-risk transactions or for changing the address of your account.'

CHIP AND PIN

One area where the banks have made a huge step forward in security is chip and Pin cards. By the

end of 2005 most credit or debit cards will use this new system. Instead of handing over your card and signing for transactions, you place your card in a reader and enter your Pin. No one else handles the card, which reduces the risk of skimming. The Pin makes it harder for people to use a stolen card.

Chip and Pin isn't a panacea. It's possible it will just shift the focus of fraud elsewhere, for example to online or other transactions when the card is not present. *'Perhaps the next big area to be tackled needs to be improving online security and checking Pins online,'* says Ken Farrow. If they don't already, online retailers should ensure that they at least ask for the three-digit security number on the signature strip on the back of your card.

Another danger is that while chip and Pin will help cut down on transaction fraud, it's irrelevant if a criminal manages to make a fraudulent application. *'If they manage to open an account in your name, there is nothing to stop them getting their own chip and Pin card, is there?'* points out Neil Munroe.

Neil goes on to say that it's not just the financial industry that needs to tackle fraud: *'Government, private companies, and consumers all need to do more to stop fraud. People need to be more aware of the actions they need to take to protect themselves. We should be talking about prevention rather than cure.'*

This is undoubtedly true. One of the government's big ideas on tackling some of these issues is the new national ID card scheme. In the meantime we all need to be careful with our personal information so we don't have to go through what Bob Armstrong suffered.

How can I stay safe? *Here are some top tips to avoid ID fraud:*

- Make sure that you are not using your mother's maiden name or place of birth as a security password.
- Check your credit file annually (and especially just after you've moved). If you change address, make sure you pass on your new details to your bank and anyone else who sends you post. You should also ask Royal Mail to redirect post.
- Don't just toss your old post straight into the bin. Rip it up burn it in the garden or buy a shredder. Be especially careful with 'pre-approved' partly filled-in bank credit forms.
- Never use the same password for more than one account. If you bank online, use a different password for other websites.
- Try not to carry details of your home address along with your bank cards in a purse or wallet. This also applies to your driving licence. Don't carry it unless you specifically need it that day. Even if you *are* stopped by the police, you have seven days to present it.