# Join the battle to beat card fraud

**Criminals are stealing £1.4 million from our accounts every day. Here's how you can avoid becoming a victim**

Organised gangs of criminals are finding increasingly sophisticated ways to use your bank account to fund serious crime and even terrorism. Yet our research shows that many people are making it easy for them simply by doing little to protect themselves against fraud.

In 2004, £500 million was lost to card fraud, an increase of 600 per cent since 1995. This is only a fraction of the huge amount spent on cards each year – a staggering £273 billion in 2004, which averages out at £5,700 for each person – but it is a growing problem that costs millions to combat.

## WHO PAYS?

Thankfully, you're not liable for fraud unless you act without reasonable care or are complicit in it. A spokesperson from Apacs (the body that runs the card system in the UK) told us: 'The most cardholders are liable for is £50 and this is rarely enforced. Consumers do not have to pay for fraud unless they are grossly negligent.' If your card is still in your possession, you are not liable at all.

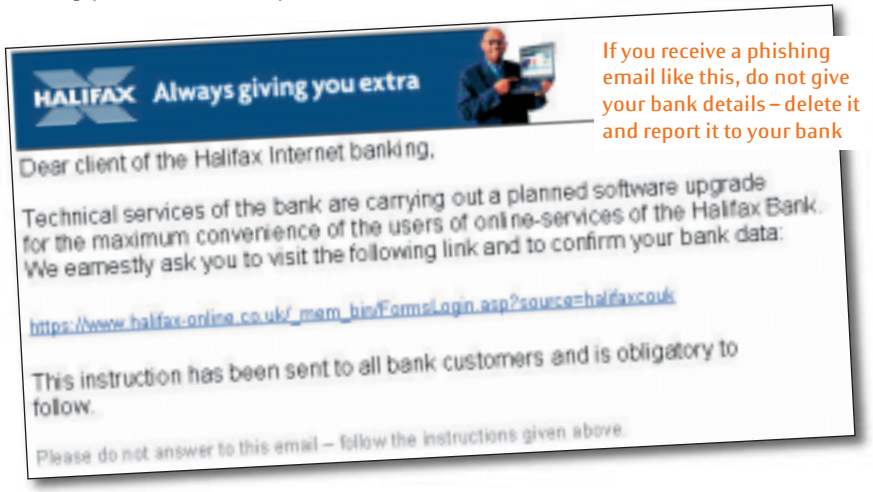
But don't let this make you complacent. Although banks swallow the costs of fraud, we all pay for it in the end through higher bank charges, interest rates and fees, as well as higher prices for goods and services. Sooner or later, banks are likely to come down harder on consumers who don't take basic precautions to protect themselves against fraud.

## HOW CRIMINALS OPERATE

Criminals don't need your bank cards to commit fraud – just the details on them. They've devised some frightening ways of obtaining this information that are now widely used.

**Phishing** When criminals send bogus emails that appear to be from a bank or card company, this is known as phishing. It started in 2003 but is now so common that the word has been added to the *Oxford Dictionary of Modern Slang*. Phishing emails (like the one below) direct you to a website to confirm or provide security details or account information. The criminals then gain access to your online account. Phishing is the easiest fraud to beat – banks or credit card companies will never ask you to go online and enter or confirm security details. Don't reply to these emails, just delete them.

Shield the keypad when entering your Pin from any hidden cameras above


HALIFAX Always giving you extra

Dear client of the Halifax Internet banking,

Technical services of the bank are carrying out a planned software upgrade for the maximum convenience of the users of online-services of the Halifax Bank. We earnestly ask you to visit the following link and to confirm your bank data:

https://www.halifax-online.co.uk/_mem_bin/FormsLogin.asp?source=halifaxcouk

This instruction has been sent to all bank customers and is obligatory to follow.

Please do not answer to this email – follow the instructions given above.

If you receive a phishing email like this, do not give your bank details – delete it and report it to your bank

**Pharming** This relies on a computer virus that automatically forwards you to a fake website when you access your online bank account. The only way to beat pharming attacks is to install, and regularly update, virus and firewall software. When you log into your online accounts check that the web address is correct before entering your details.

**Skimming** The most common type of cash-machine fraud is 'skimming'. This is where criminals attach card readers, such as the one pictured below, to cash machines. These capture your card details. Small cameras are also installed that film your hand keying in your Pin. The criminals then make a counterfeit copy of your card and use your Pin to withdraw your cash with it.


These devices are becoming smaller, more sophisticated and harder to spot. If a cash machine looks suspicious, don't use it, but report it to the police and the bank instead. Always use your hand to shield the keypad from cameras when you enter your Pin.

**Stealing in transit** Millions of credit and debit cards are sent out to customers each year – 8.7 million new chip and Pin cards were sent out in August alone. Inevitably, some are stolen in transit.

Banks and card companies use a variety of methods to ensure that cards reach their customers – for example, by sending them by registered post or in disguised packages. But sometimes they are stolen by people who work for the banks, Royal Mail or by couriers who are wise to these disguises. Sending cards out unactivated is a good security ploy as the cardholder has to contact the bank to confirm receipt and disclose security details to activate the card. But not all banks do this.

## BANKS AND RETAILERS

There are other key things that banks and retailers could do to help prevent fraud. These include:

**Obscuring specific card details on receipts** By next summer all retailers will have to partially obscure some of the card numbers printed on receipts. But not all retailers will block out the same numbers, so fraudsters can still piece together a card's details using several receipts.

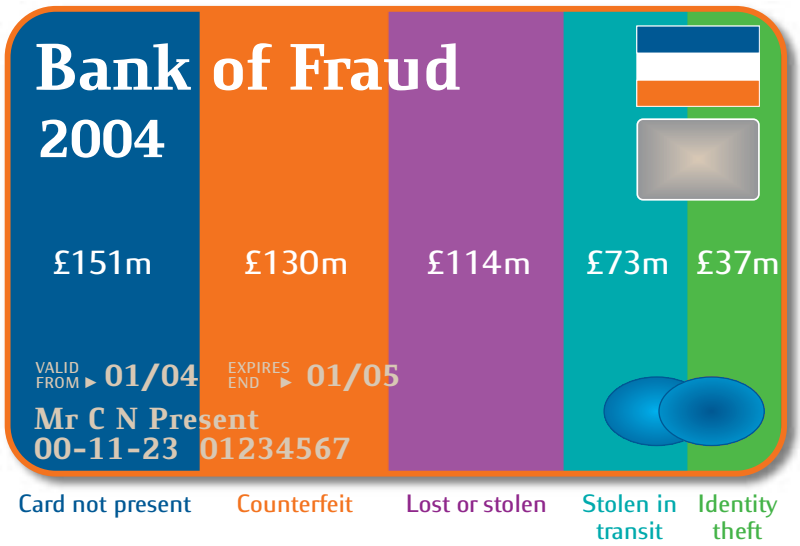
**Making proper security checks** Retailers don't always ask for the three-digit security number on the back of cards when people shop online or by phone. Doing so ensures you actually have the card and not just its details taken from a receipt or bank statement, for example. Similarly, retailers don't always check addresses to confirm that the billing address matches the cardholder's.

**Blocking cards when unusual spending occurs** Banks and credit card companies use sophisticated computer systems to spot fraudulent or unusual patterns of activity on accounts. When a bank spots a suspicious transaction, it puts a block on the card and tries to contact you. However, if you're on holiday, it may not be able to get hold of you, as banks don't always ask for mobile phone numbers.

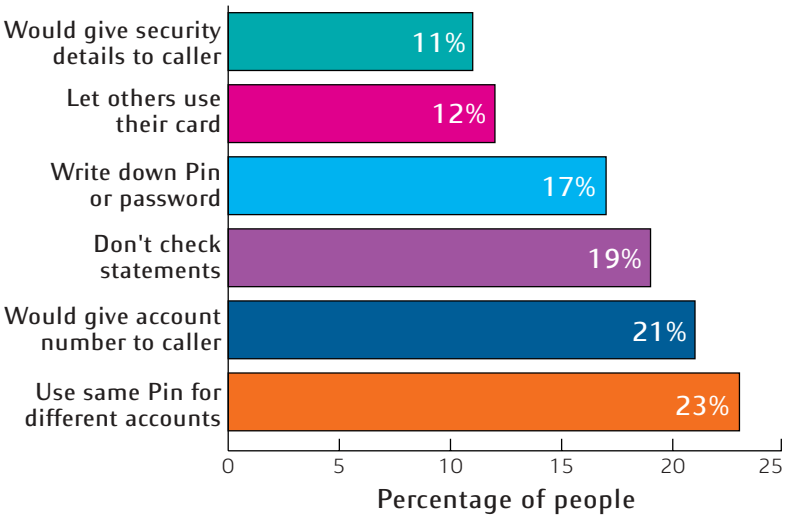
# Types of card fraud

Around 500 million was stolen through card fraud last year. Here's how:

- **Card not present** Criminals use your card details to buy things by phone, internet or mail order.
- **Counterfeit** Fraudsters use your card details to make fake cards.
- **Lost or stolen** Criminals use cards they steal or find.
- **Stolen in transit** Cards that never arrive at the card-holders' addresses because they're stolen by employees of the banks, Royal Mail or couriers, or by people in shared addresses, such as flats.
- **Identity theft** Fraudsters obtain sufficient information about you, such as your date of birth and address, to enable them to open new credit cards or bank accounts in your name.




# How we make it easy for fraudsters




In August we surveyed 1,624 adults with a current account or credit card. We found that 6 per cent of current account holders and 5 per cent of credit card holders have been victims of fraud in the last year. But is it any wonder when the graph above shows how many of you are careless when it comes to card security?

## DCI Cook: Bringing the fraudsters to justice

The Dedicated Cheque and Plastic Crime Unit (DCPCU), which is funded by banks and the Home Office, was set up in 2002 to investigate organised card fraud.

DCPCU head, Detective Chief Inspector Roger Cook, told us: 'Card fraud is big business. Most card fraud is carried out by organised gangs and is often used to fund other illegal operations, such as buying drugs or weapons, and to fund terrorism or launder money.

'Since the DCPCU was formed, we've recovered thousands of counterfeit cards and prosecuted scores of criminals, potentially saving millions of pounds. Most of the stolen card numbers and bank account details we've come across have been obtained from the internet. Hackers are a big problem.

'The last thing the criminals want to do is actually meet their victims. So there's little danger that you'll come face to face with a criminal. For example, it's extremely unlikely that someone will "shoulder surf" you while you're keying in your Pin and then steal your card.

'If you see anything suspicious on an ATM, don't touch it as you might destroy valuable forensic evidence. Just inform the police and the bank.

'Criminals will always exploit the weakest link in any security system. We have already seen a shift away from counterfeit card fraud in the UK and Europe because of chip and Pin, but we expect to see more fraud with UK cards in the US, where chip and Pin isn't used.

'To some extent you can't stop yourself being the victim of fraud, but there are lots of simple things you can do to help reduce the risk.'

DCI Cook holding up the front of a cash machine used for skimming

Always take card contact numbers or email details with you so that you can contact your card company if your card is blocked.

**Giving clear security information** Banks advise customers not to give their card details to anyone who calls or emails claiming to be from their bank, in case they are fraudsters. But, confusingly, banks themselves call customers asking for bank details when they want to sell something, or to confirm a rogue transaction.

If banks are going to do this, they should prove that they're genuine, for example, by telling you isolated parts of your password. If you aren't sure the call is genuine, take their name and call them back on your bank's normal contact number.

### EXTRA CARD SECURITY

MasterCard and Visa have joined forces with some card companies, such as Barclaycard, to introduce systems that make shopping online more secure. They're called 'SecureCode' and 'Verified by Visa' respectively, and you register your credit card to join them. Then, each time you buy from a retailer that is also signed up, you enter a password.

Jennifer Saunders promoting Barclaycard's 'SecureCode' card system

These extra security measures are welcome, but don't choose a credit card simply because of them. You aren't liable for fraud with any credit card if it's still in your possession. It's much more important to choose a credit card with a good rate. We'll name our Best Buy credit cards next month.

## PRECAUTIONS AGAINST CARD FRAUD

**Follow these steps to help reduce your likelihood of falling victim to card fraud.**

- Never divulge full details of your password or Pin to callers who say they are from your bank or the police.
- **Guard your cards and card details. If possible, don't let cards out of your sight when you pay.**
- Regularly check statements for suspicious transactions.
- **Get credit files from all three credit reference agencies every six to 12 months to check for any fraudulent activity, such as credit searches or new accounts. (See our report on credit cards next month for more on credit reference agencies.)**
- Cut up and dispose of old cards and cheque books and cancel them with your bank or card issuer.
- **Keep a note of contact details to use if your card is lost or stolen. Carry them separately from your bank cards and report any lost or stolen cards immediately.**
- Dispose of card receipts and other financial documents carefully by shredding them – see 'Shredders', p60, for our Best Buys.
- **When using cash machines, use your hand to shield your Pin from any hidden cameras above the keypad. If anything about the machine looks odd, don't use it. Report it to the bank and the police.**
- Avoid obvious Pins such as your birth year. For ideas on ways to remember Pins, see www.chipandpin.co.uk

### ONLINE TIPS

- Be wary of sharing PCs – always log off properly from sites and web browsers.
- **Shop only on sites with the padlock symbol and https, not http, in the address.**
- Install virus and firewall software to protect against hackers and fraudsters, and make sure you update it regularly.
- **Never respond to emails, or use links from emails, asking you to confirm security or bank details. They are false.**
- Always check the web address of your bank is correct before you enter any details.
- **Use the latest versions of internet and browser software and set firewalls to the highest levels of security available.**

PHOTOGRAPHY JOHN TRENHOLM