Fraud
The Facts 2006

The definitive overview of plastic card, cheque and online banking fraud – and measures to prevent them

APACS

APACS – the UK payments association – is the trade association for payments and provides the forum for the UK's financial institutions to come together on non-competitive issues. It is also the banking industry voice on payment issues such as plastic cards, card fraud, cheques, electronic payments and cash.

Two of our main fraud prevention committees are the Fraud Control Steering Group and the Plastic Fraud Prevention Forum:

"Card and cheque fraud losses both decreased during 2005, whilst online banking fraud losses increased. This clearly demonstrates that we cannot relax our guard in the fight against all types of payment fraud, as the organised criminal gangs responsible will continue to target any perceived weakness in our defences.

However, we have proved through the effectiveness of such anti-fraud initiatives as chip and PIN and the Dedicated Cheque and Plastic Crime Unit that we are fully committed to tackling payment fraud in all its forms and we will continue to work with all banking industry stakeholders to explore and implement other appropriate fraud prevention solutions.

In addition, our work with the retail industry, law enforcement and the Home Office will continue to look at both short-term and long-term solutions in the battle against those responsible."

Joint statement from **Paul Baker**, chairman of the Fraud Control Steering Group, and **Derek Wylde**, chairman of the Plastic Fraud Prevention Forum.

Plastic card fraud

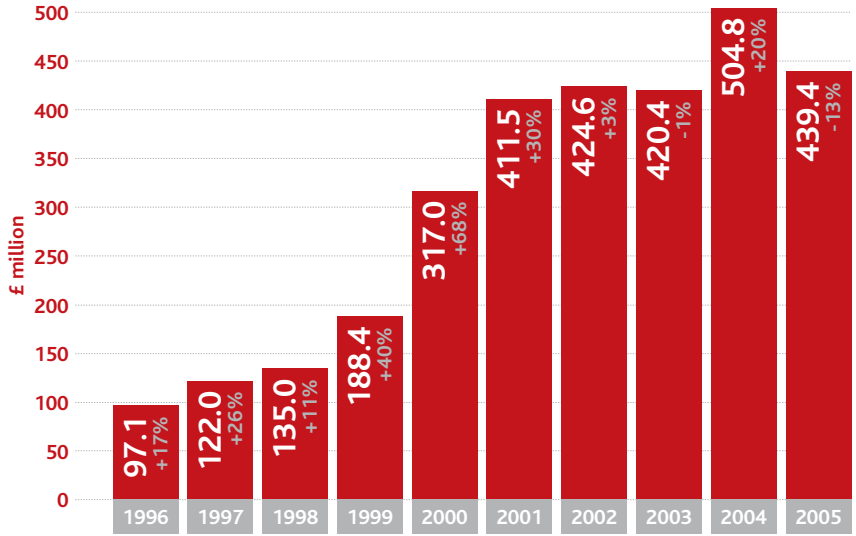
4 Overview and types of plastic card fraud

23 Preventing plastic card fraud

33 Cardholder advice

Plastic card fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Annual plastic card fraud losses on UK-issued cards 1996-2005

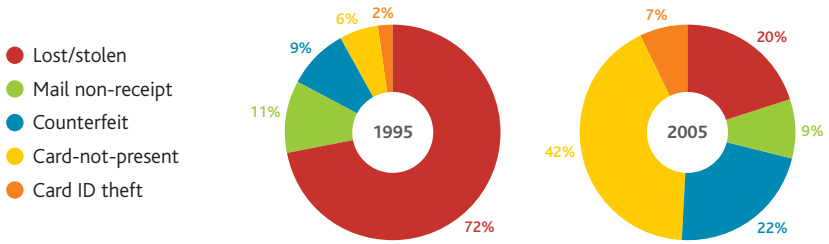
All figures in £ millions

Fraud type	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Card-not-present	6.5	10.0	13.6	29.3	72.9	95.7	110.1	122.1	150.8	183.2
Counterfeit	13.3	20.3	26.8	50.3	107.1	160.4	148.5	110.6	129.7	96.8
Lost/stolen	60.0	66.2	65.8	79.7	101.9	114.0	108.3	112.4	114.5	89.0
Mail non-receipt	10.0	12.5	12.0	14.6	17.7	26.8	37.1	45.1	72.9	40.0
Card ID Theft	7.2	13.1	16.8	14.4	17.4	14.6	20.6	30.2	36.9	30.5
Total	97.1	122.0	135.0	188.4	317.0	411.5	424.6	420.4	504.8	439.4

Overview

Whilst card usage and transaction volumes continue to grow, plastic card fraud losses against total turnover – at 0.112% – are significantly less than the 1991 peak level of 0.33%. This fraud-to-turnover ratio fell by 21% from 0.141% in 2004.

Card fraud losses split by type (as percentage of total losses)



* (See table on page 7) Fraud losses in all but one of the regions reflect what is happening at a national level – CNP fraud is rising, but the other fraud types are falling so much that the overall effect leads to a drop in total card fraud.

In Yorkshire and Humberside, however, CNP fraud losses have increased by 69% – which is greater than the decreases seen in the other fraud types and has caused an overall increase for that particular region. The CNP fraud increase in Yorkshire & Humberside is due to a combination of factors but is most probably influenced by the fact that a large amount of CNP transactions are processed in Yorkshire & Humberside (i.e. the head offices of large CNP merchants are based in the region). It is not necessarily because CNP fraudsters are targeting cardholders in this particular region.

Plastic card fraud losses in the UK in 2005 on UK-issued cards split by UK region

Region	2005 (+/- change)	2004	2003
South East *(includes Greater London)*	£208.7m (-13%) *£130.0m (-26%)*	£239.3m *£176.5m*	£184.4m *£134.4m*
North West	£29.6m (-23%)	£38.4m	£24.8m
Yorkshire & Humberside*	£27.8m (+16%)	£24.0m	£17.7m
East Midlands	£23.5m (-23%)	£30.7m	£19.0m
West Midlands	£21.4m (-14%)	£25.0m	£22.9m
Scotland	£14.1m (-16%)	£16.7m	£14.7m
South West	£11.3m (-11%)	£12.7m	£11.3m
North East	£7.5m (-07%)	£8.1m	£6.7m
East Anglia	£6.6m (-27%)	£9.0m	£6.9m
Wales	£5.3m (-28%)	£7.3m	£6.6m
Northern Ireland	£0.8m (-24%)	£1.1m	£1.3m
UK total	£356.6m (-13%)	£412.3m	£316.3m
Fraud abroad	£82.8m (-11%)	£92.5m	£104.1m
Total all UK cards	£439.4m (-13%)	£504.8m	£420.4m

Card-not-present (Internet, phone and mail order) fraud

£183.2m in 2005 (up 21%)

Card-not-present (CNP) fraud involves the use of stolen card details in non face-to-face transactions either on the Internet, by phone or by mail order. It has been the largest type of card fraud in the UK for the past three years. The rate of increase, however, decreased last year for the first time since 2003.

The difficulty in countering this type of fraud lies in the fact that neither the card nor the cardholder is present when the transaction happens. This means that:

- Businesses accepting these transactions are unable to check the card's physical security features to determine if it is genuine;
- Without a signature or a PIN there is less certainty that the customer is the genuine cardholder;
- Card companies cannot guarantee that the information provided in a card-not-present environment has been given by the genuine cardholder.

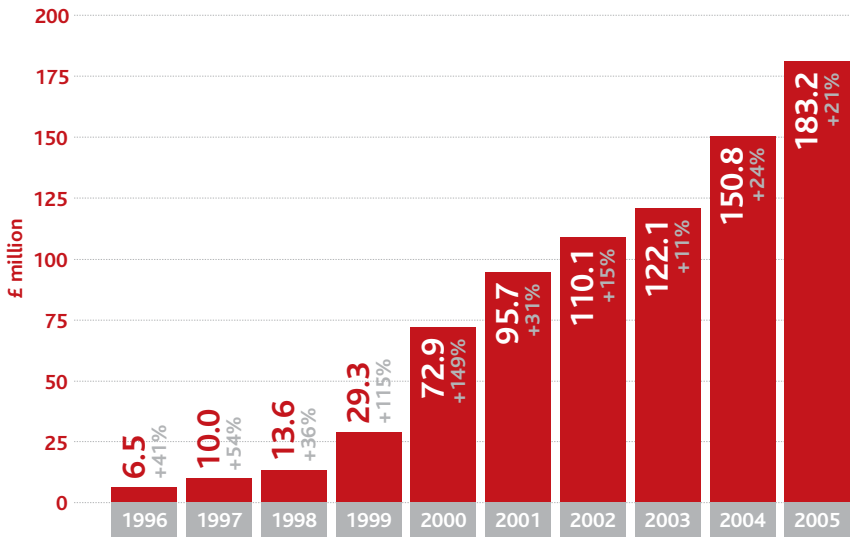
A number of initiatives are available to help businesses protect themselves from card-not-present fraud (see page 27).

What is card-not-present fraud?

This crime most commonly involves the theft of genuine card details in the real world that are then used to make a purchase over the Internet, by phone, or mail order. The legitimate cardholder may not be aware of this fraud until they check their statement.

Card-not-present fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Counterfeit card fraud £96.8m in 2005 (down 25%)

The main reason for the fall in counterfeit card fraud is the introduction of chip and PIN in the UK. Counterfeit card fraud losses are now at their lowest level since 1999.

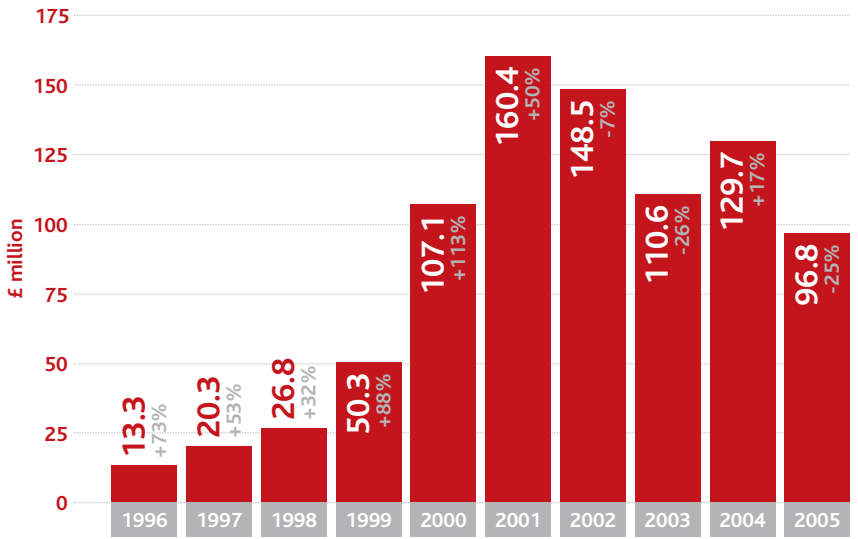
What is counterfeit card fraud?

Counterfeit card fraud occurs when an illegal copy of a genuine credit or debit card is made. Most cases of counterfeit fraud involve skimming, whereby the data on a genuine card's magnetic stripe is electronically copied onto the magnetic stripe of another card, without the legitimate cardholder's knowledge.

Skimming typically occurs in places where a corrupt employee electronically copies the magnetic stripe of a customer's card before handing it back, then sells the information on higher up the criminal ladder where counterfeit magnetic stripe cards are made. Often cardholders are unaware of the fraud until a statement arrives showing purchases they did not make. Since mid-2003, organised criminal gangs have adapted skimming devices for use at cash machines.

Counterfeit fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Lost and stolen card fraud £89.0m in 2005 (down 22%)

Thanks to the introduction of chip and PIN this type of card fraud is now at its lowest level since 1999.

As well as the proven security benefits of chip and PIN, the banking industry has a number of other initiatives in place to tackle this type of fraud:

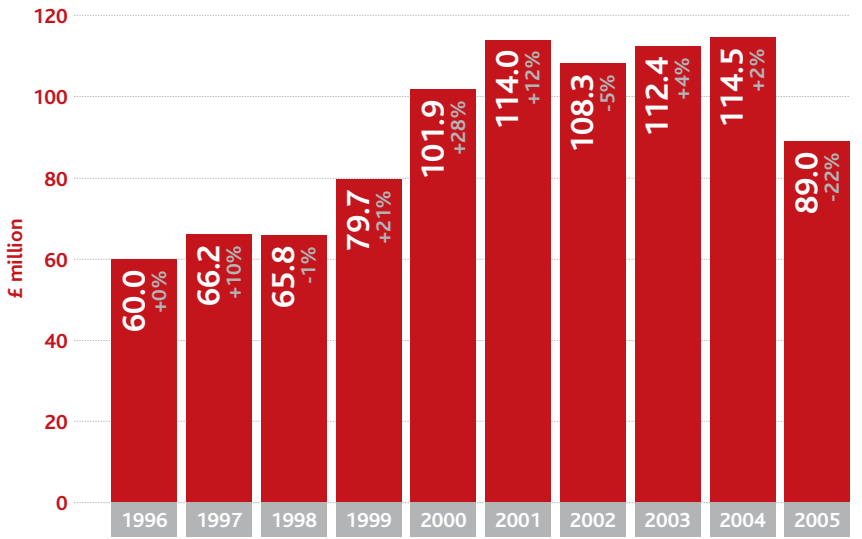
- A retailer education programme, run by APACS since 2001, provides help for shop staff on how to detect stolen and counterfeit cards at the till point. An online version of this retailer-training programme is available at **www.cardwatch.org.uk**
- Card company use of intelligent computer systems that track customer accounts for unusual spending patterns.
- An Industry Hot Card File (see page 32) enables retailers to electronically check whether a card has been reported lost or stolen.

What is lost and stolen card fraud?

This category covers fraud on cards that have been reported by the cardholder as lost or stolen. Most fraud in this category takes place in shops without chip and PIN equipment, before the cardholder has reported the loss.

Lost and stolen fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Mail non-receipt fraud £40.0m in 2005 (down 45%)

This type of fraud decreased 45% to £40.0m in 2005, representing less than 10% of total fraud losses. The main reason behind this large decrease is the introduction of chip and PIN, mostly because it has become more difficult for fraudsters to use stolen cards without the PIN, but also because less cards are being sent out than at the peak of the chip and PIN roll-out.

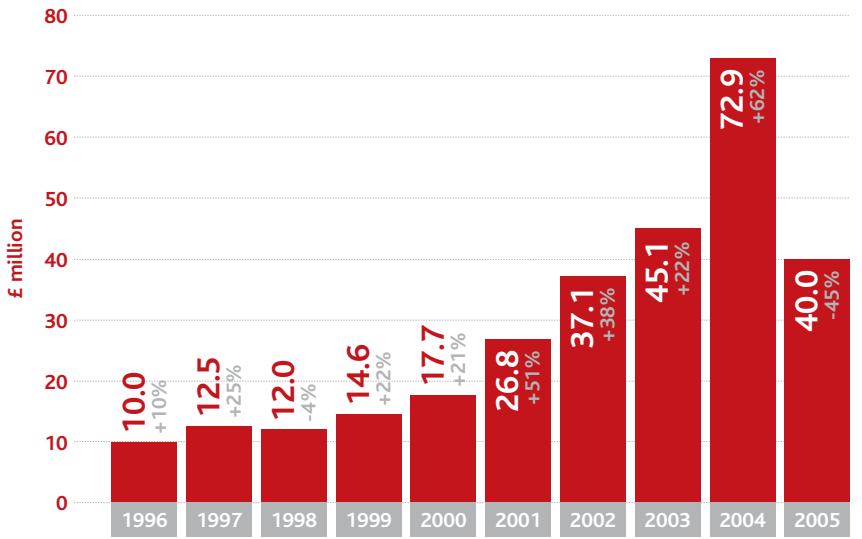
In addition, the banking industry continues to work with the Royal Mail and other organisations it uses to deliver its cards to monitor card losses, identify fraud hot spots and take preventative action. Customers may be required to phone their card companies before cards can be used. Card companies may use secure couriers to deliver to high-risk postcodes or cards may be sent to a customer's branch for personal collection.

What is mail non-receipt fraud?

This type of fraud involves cards being stolen in transit – after card companies send them out and before the genuine cardholders receive them. Particularly at risk for this type of fraud are properties with communal letterboxes, such as flats and student halls of residence.

Mail non-receipt fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Card ID theft £30.5m in 2005 (down 17%)

Although identity theft is often referred to as "Britain's fastest growing crime", card ID theft has fallen by 17% in the past year and currently accounts for less than 7% of overall card fraud losses.

What is card ID theft?

Card ID theft occurs when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over a card account in someone else's name. There are two types:

Application fraud £12.4m in 2005 (down 5%)

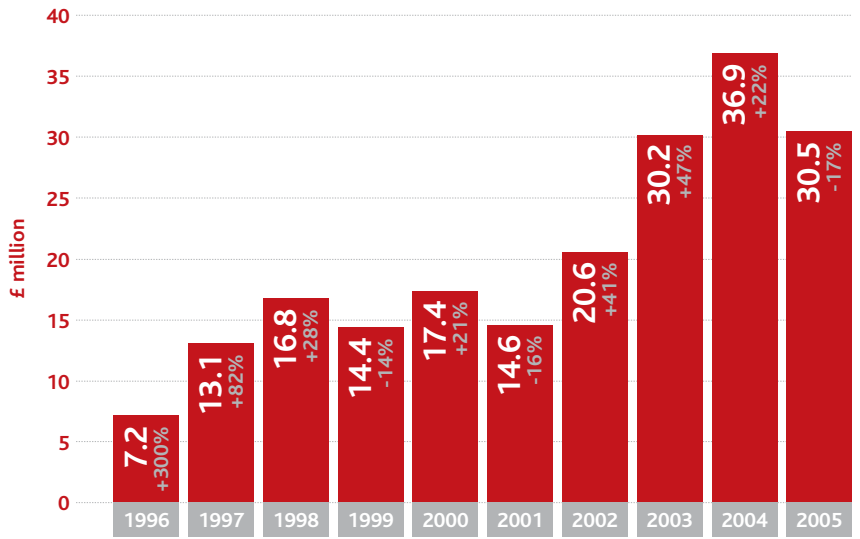
Application fraud involves criminals using stolen or false documents to open an account in someone else's name. Criminals steal documents such as utility bills and bank statements to build up usable information. Alternatively, they may use counterfeit documents for identification purposes.

Account take-over £18.1m in 2005 (down 24%)

Criminals use fraudulently obtained personal financial information and card details to deceive a bank or card company into believing they are the genuine cardholder. They then take over and start accessing the cardholder's account. In a typical situation they will also change the address on the account, and ask for new cards and chequebooks to be sent out.

Card ID theft on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Where does card fraud take place?

Although a large amount of card fraud occurs in shops and businesses in the UK, other locations for card fraud include cash machines and fraudulent transactions made overseas on UK-issued cards:

Cash machine fraud £65.8m in 2005 (down 12%)

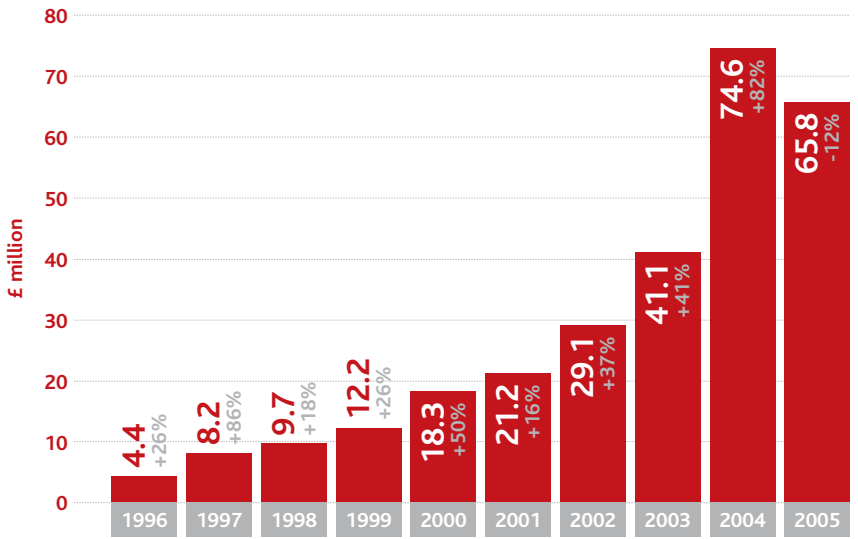
Cash machine fraud is not a type of fraud but describes the location where it occurs. Fraud at cash machines in the UK decreased by 12% last year and now accounts for less than 15% of total plastic card fraud losses.

Criminals commit fraud at a cash machine in a number of ways:

- Skimming from the magnetic stripe at cash machines – a skimming device is attached to the card entry slot to record the electronic details from the magnetic stripe of genuine cards as they are inserted into the cash machine and a miniature camera is hidden overlooking the PIN pad to capture the PIN being entered. This enables the criminal to produce a counterfeit magnetic stripe card, which is then matched up with the genuine PIN.
- Shoulder surfing – criminals look over a cardholder's shoulder to watch the PIN being entered, then steal the card using distraction techniques or pickpocketing, before using the stolen card and genuine PIN.
- Card-trapping devices – a device, inserted into a cash machine's card slot, retains the card inside the cash machine. The criminal tricks the victim into re-entering the PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.
- Customers who have written down their PINs – a cardholder writes down their PIN and keeps it in their purse or wallet, which is then lost or stolen.

Cash machine fraud losses on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Fraud abroad £82.8m in 2005 (down 11%)

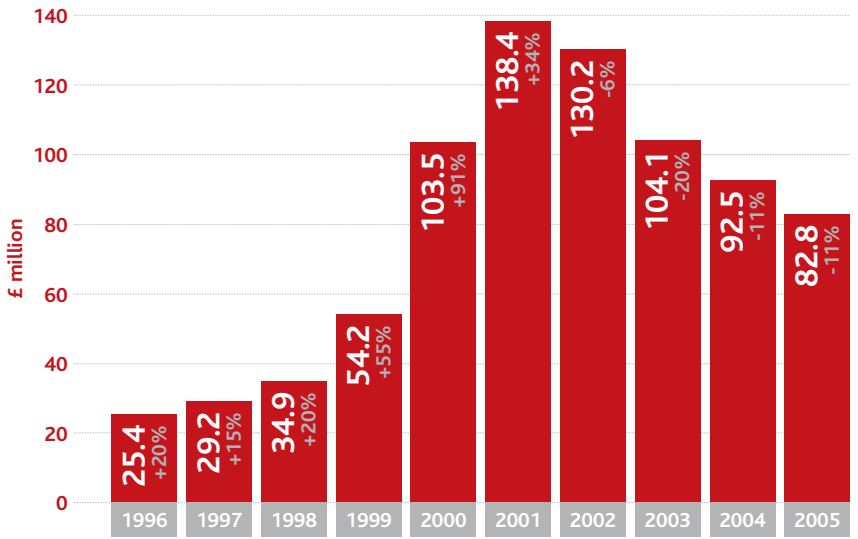
Card fraud losses that occur overseas on UK-issued cards have decreased for the fourth consecutive year. Fraud abroad now accounts for just under one-fifth of fraud (19%) on UK cards. Since 2001 fraud abroad has declined by 40%. The main reasons for the reduction in fraud abroad are:

- Card companies' increased use of intelligent fraud-detection systems;
- The work of the banking industry-sponsored specialist police unit (see page 25), which has cracked several counterfeiting groups with international links.

Over one-third (40%) of fraud abroad took place in three countries. France accounted for 14% (£11.6m) of losses on UK cards used abroad; USA 14% (£11.2m); and Spain 12% (£9.5m). Although part of these losses are the result of British holidaymakers having their cards stolen whilst abroad, the majority of this fraud is the result of fraudsters using card details stolen in the UK.

Fraud committed abroad on UK-issued cards 1996-2005

Figures in grey show percentage change on previous year's total



Internet/e-commerce fraud estimated at £117.1m in 2005

Internet fraud on cards is part of the CNP total of £183.2 million. In 2005 the amount of CNP fraud that took place over the Internet is estimated at £117.1 million – 64% of total CNP losses. This figure is virtually unchanged from 2004, when Internet losses were £117.0 million, although last year this represented 78% of CNP losses.

The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, bin-raiding or through unsolicited e-mails or telephone calls. The card details are then used to make fraudulent card-not-present transactions, most commonly via the Internet. The incidence of computer hackers stealing and using cardholder data from websites is very low.

However, as the opportunities for online commerce have increased so, unfortunately, has criminal interest. Spam e-mail gives the fraudsters an easy way of contacting millions of Internet users around the world, regardless of their physical location, to try to dupe them into disclosing valuable personal information that could be used to commit all types of identity theft or to get their card details that can then be used to make fraudulent purchases.

Advice for businesses on how to protect themselves from this type of fraud is detailed on page 27.

Chip and PIN

Making card transactions safer

Chip and PIN has been the biggest change to the way we pay since decimalisation and is part of a global programme to tackle plastic card fraud.

It combines two effective security features. The first, the chip or microchip on the card stores card data more securely than the magnetic stripe, making chip and PIN cards much harder to counterfeit. The second is the four-digit PIN (personal identification number), which is used to prove you are the genuine cardholder. It is a much safer way to prove you are the genuine cardholder as a PIN, unlike a signature, is not written on the back of the card.

The final phase of the national roll-out was achieved on Valentine's Day 2006. Since this date cardholders with a chip and PIN card have needed to know the PIN on their chip and PIN card to be sure that they can use that card. If they do not know the PIN, the card may be declined and they should not expect to be able to sign. Some exceptions still exist where people continue to sign:

- Cardholders with old-style cards.
- Cardholders from other countries with old-style signature cards that have not yet been upgraded to chip and PIN.
- Cardholders who are unable to use a PIN because of a disability who have been issued with a chip and signature card.
- Cardholders in shops that have not upgraded to chip and PIN.

A UK success story

The UK has led the world in implementing the global standard for chip and PIN. APACS and its members were instrumental in the development of this standard, and the UK's chip and PIN roll-out is more advanced than any other country in the world. As a result, UK cardholders will be safer using their cards not just at home, but also increasingly throughout Europe, Asia, the middle-East, the far-East, Australasia and Central and Latin America as they upgrade their systems.

More information about chip and PIN can be found at **www.chipandpin.co.uk**

Why not photo cards instead of PINs?

Putting photographs on cards would still rely on the retailer taking responsibility for identifying the cardholder. With the introduction of PINs, the responsibility of identifying the cardholder moves away from retail staff to a more secure, technology-based method.

What about identification methods like iris scanning?

The memory capacity of the chip on the card makes it possible to retain biometric details to identify the cardholder. Finger and iris scanning as well as voice recognition and dynamic signature have all been put forward as possibilities. Such technology is not yet sufficiently reliable or cost-effective in a retail environment to meet the requirements of the UK card industry.

Dedicated Cheque and Plastic Crime Unit (DCPCU)

A specialist police unit targeting organised criminal gangs

APACS, the Association of Chief Police Officers (ACPO) and the Home Office launched the DCPCU in April 2002 as a two-year pilot to tackle the organised criminal gangs responsible for the majority of cheque and plastic card crime in the UK.

Following the successful conclusion of the pilot, the Unit was then established as a permanent body and is now, uniquely, sponsored by the banking industry.

Since its inception the DCPCU has achieved in excess of £100 million of potential savings to the banking industry through the recovery of hundreds of thousands of counterfeit cards and compromised card numbers.

The Unit is jointly resourced, with APACS and its members providing fraud investigators and administrators who work alongside officers from the City of London and Metropolitan Police.

Fraud Intelligence Bureau (FIB)

Exchanging information to fight fraud

The FIB distributes information and intelligence between the banking industry, police forces and other law enforcement agencies throughout the UK to combat card fraud. It has helped identify several major counterfeiting rings run by organised criminals.

The FIB, which works closely with the DCPCU, is developing its role to extend the intelligence it collects on other card fraud types – including card-not-present, account takeover and mail non-receipt – and also non-plastic fraud data.

Fighting card fraud in the retail environment

Training shop staff to stop fraud

There has been a significant reduction in card fraud losses on face-to-face transactions in UK shops and businesses, down 38% to £135.9 million. Much of this is down to the introduction of chip and PIN. However, a small percentage of businesses have yet to upgrade to this new technology and APACS continues to work with these retailers, using its *Spot & Stop Card Fraud* education pack and training programme. Developed in collaboration with retailers, police and organisations including Crimestoppers, it helps retail staff identify counterfeit and stolen plastic cards.

An online version of the training pack and a DVD to complement the training programme is available at **www.cardwatch.org.uk**.

Spot & Stop Card Fraud is part of a wider, ongoing retailer education programme that incorporates a range of free publications.

Systems to reduce CNP (Internet, phone and mail order) fraud

Helping businesses fight card-not-present fraud

Although card-not-present fraud is increasing, these losses must be set against the phenomenal increases in both the volume and value of these types of transaction as more and more businesses offer online and telephone methods of payment.

A number of initiatives are in place to counter this type of fraud:

- An automated cardholder address verification and card security code (AVS/CSC) system is available for businesses that accept card-not-present transactions. The system allows them to verify the billing address of a cardholder and cross-check the security code on the signature strip of the card. These data checks provide additional information to help businesses assess fraud risks and decide whether to proceed with the transaction.
- Visa and MasterCard have introduced secure payment systems (*Verified by Visa* and *MasterCard SecureCode*) for safer online transactions. (**www.visaeurope.com/verified** and **www.mastercard.co.uk/securecode**)
- Retailers are also encouraged to make use of various card-not-present fraud prevention tools, such as intelligent fraud detection software, available from third-party providers.
- APACS' *Spot & Stop Card-not-Present Fraud* provides comprehensive fraud prevention training for card-not-present businesses. An e-learning version is available at **www.cardwatch.org.uk.**
- APACS facilitates a cross-sector working group – involving banks, retailers, card schemes, law enforcement and trade associations – which continues to work on system enhancements and new developments to combat card-not-present fraud.

Using chip and PIN to make non face-to-face transactions safer

Hand-held card readers that create one-off passcodes

The next stage in the development of making card-not-present payments safer is to build on the security benefits of chip and PIN through the use of a token-based authentication system. A token-based system uses something you have – the token (i.e. your card) – and something you know – such as a password or PIN.

The system would work via a hand-held card reader, into which a chip and PIN card is inserted. The user then enters their PIN and the one-time only passcode is generated, which the customer provides to the merchant, when prompted, to authorise the transaction.

The industry has developed a UK standard to ensure that the card readers are interoperable, which would allow any UK chip and PIN card to be used in any reader. This would ensure that people with a number of credit cards would only need one reader.

Banks' use of intelligent fraud-detection systems

Checking for unusual spending patterns to spot fraud before it is reported by the cardholder

Card companies continue to increase the effectiveness and sophistication of customer-profiling neural network systems that can identify at a very early stage unusual spending patterns and potentially fraudulent transactions. The card company will then contact the cardholder to check if the suspect transaction is genuine. If not, an immediate block can be put on the card.

These systems identify suspect transactions taking place both in the UK and internationally with considerable success.

Prevention of card ID theft

Cross-industry co-operation to fight card ID theft

Although card ID theft is decreasing in the UK measures will remain in place and will continue to be developed to combat this type of fraud.

In 2002 APACS set up a multi-sector working group to tackle this type of fraud, involving the British Bankers' Association, CIFAS, key government departments and law enforcement bodies.

This has resulted in a number of initiatives:

- APACS published *Identity Fraud – the UK Manual* in conjunction with CIFAS and the Finance & Leasing Association with the support of the Home Office. *The Manual* includes a training programme and best practice guidelines, explaining how businesses and organisations can best protect themselves and their customers.
- **www.idfraudpreventiontraining.com** is an online training site for businesses, developed by APACS, the British Bankers' Association and CIFAS, with Home Office backing.
- A Home Office Identity Fraud Steering Committee, consisting of senior representatives from the public and private sectors, including APACS, brings together all those with an interest in reducing identity fraud in the UK.
- APACS played a key role in the development of **www.identitytheft.org.uk** – a consumer-focused website launched by the Home Office. It advises the public how best to protect themselves from identity theft and has advice for victims. This has now been complemented with a range of leaflets and posters for use in public areas including libraries, Citizens Advice Bureaux and bank counters.

Preventing fraud on the Internet

Secure methods to prevent online fraud

Most Internet fraud occurs after card details have been fraudulently obtained in the real world. Typically this might involve corrupt employees in pubs and restaurants copying card details when cards leave the cardholders' sight, or criminals stealing carelessly discarded financial information.

The international card schemes have launched new security measures to prevent criminals using other people's card details online. *Verified by Visa* and *MasterCard SecureCode* enable cardholders to use a private passcode to authenticate themselves when shopping online at participating merchants. The systems also allow financial institutions to confirm a cardholder's identity for the merchant when a genuine customer is using their card online. Enabling merchants to confirm cardholder identity in this way puts another barrier between criminals and cardholder information. These systems also have the advantage of being global, which helps tackle fraud abroad.

Further details about *Verified by Visa* and *MasterCard SecureCode* can be obtained from **www.visaeurope.com/verified** and **www.mastercard.co.uk/securecode**

For both Internet and the more traditional forms of card-not-present fraud the possible roll-out of token-based authentication could help to reduce losses, primarily in the UK but also potentially across Europe (see page 28).

Preventing cash machine fraud

Multi-layered approach to tackling fraud

A number of initiatives are ongoing to counter cash machine fraud including:

- Chip and PIN, which effectively combats the use of skimmed cards in cash machines;
- Making cash machines tamper-proof so that skimming devices either cannot be fixed to cash machines or do not work when they have been fixed;
- Installing CCTV cameras and siting cash machines in well-lit locations to deter fraudulent activity;
- Continued liaison with the police;
- Placing a safety zone or defensible space around the machine (a marked area on the pavement for only the cash machine user to stand in);
- Raising awareness to cash machine users of best practice advice.

CIFAS – the UK's Fraud Prevention Service

Sharing information to stop fraud

CIFAS is a fraud prevention body that provides a range of services enabling its members to share information relating to fraudulent activity, with the aim of helping to identify and prevent fraud, including that relating to plastic cards.

See **www.cifas.org.uk** for more information.

Industry Hot Card File (IHCF)

Checking every card transaction for cards being used fraudulently

More than 80,000 retailers subscribe to this electronic file that provides information on lost and stolen cards. When a participating retailer accepts a card payment as part of a normal transaction, it is automatically checked against the file and the retailer is alerted if the card's details match those on file.

The IHCF contains information on more than 6 million missing cards and over 430,000 cases of attempted fraud were prevented by this system in 2005.

The IHCF is being used successfully at motorway tollbooths in France to combat the use of stolen UK cards at road tolls and a project is also under way to establish their use at tollbooths in Spain.

General Advice

- Don't let your cards or your card details out of your sight when making a transaction.
- Check receipts against statements carefully. If you find an unfamiliar transaction, contact your card company immediately.
- Never write down your PIN and never disclose it to anyone, even if they claim to be from your bank or the police.
- When you dispose of them tear up, or preferably shred, any documents or receipts that contain information relating to your financial affairs.
- Report lost or stolen cards or any suspected fraudulent use of your card to your card company immediately. The 24-hour emergency number is on your last statement or call directory enquiries.

When making phone transactions using your credit, debit or charge card:

- Don't give your card details over the phone to cold callers. Only make telephone transactions when you have instigated the call and are familiar with the company.
- Have the card in front of you. You will be asked for information including the account number and expiry date. Additionally you will increasingly be asked for the three or four-digit card security code on the signature strip, issue number, your name as it appears on your card and the address as it appears on your card statement. Never give your PIN to anyone.
- Always ask the retailer to confirm the full price to be charged to your card, including any booking fees, delivery charges etc. Keep a note of these details.
- If the retailer sends you written confirmation of the order, check the bill to ensure that it is correct. Keep any such receipts and check them off against your next statement.

When shopping online:

- Sign up to *Verified by Visa* and *MasterCard SecureCode* on a retailer's or your card company's website. By signing up you will be further safeguarding your card details from online misuse.
- Only shop at secure websites – ensure that the security icon (the locked padlock or unbroken key symbol) is showing in the bottom of your browser window before sending your card details. The beginning of the retailer's Internet address will also change from 'http' to 'https' when a purchase is made using a secure connection. Use sites you can trust, for example sites you know or that have been recommended to you.
- Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to seek redress if problems arise, but having all the aforementioned information will help your card issuer take up your case if you subsequently have any difficulties.
- Ensure you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments.
- If you regularly make transactions over the Internet consider using a separate credit card specifically for these transactions.
- More tips concerning how to protect your computer from fraudulent activity can be found in the online banking fraud section on page 49.

Advice when choosing a PIN:

- To remember a new PIN you could use an anniversary or a friend's birthday. Use a combination of day and month or month and year – but don't use numbers that are easily associated with you, like your own date of birth.
- Ideally choose a random combination of numbers – this is the hardest for a criminal to guess. If this is difficult for you to remember then perhaps use the year that you left school or the number of letters in a four-word phrase that you can easily remember (e.g. *'keep this a secret'* would equate to 4416).
- Rather than remembering a PIN digit-by-digit, learn the pattern that you need to trace on the keypad with your fingers. All keypads are configured in the same way, so by remembering a square formation on the outside of the keypad that begins with '1' and moves in a clockwise direction, your number would be 1397.

Keeping your PIN a secret:

- Don't allow anyone else to use your card, PIN or other security information. Never write down or record your PIN or other security information.
- When entering your PIN use your spare hand or your body to shield the number from any prying eyes or hidden cameras. If you think someone has seen your PIN you can change it at a cash machine.
- Memorise your PIN and other security information and destroy the notification as soon as you receive it. If the PIN you are given is difficult to remember, change it to something more memorable at a cash machine as soon as possible.
- Always take reasonable steps to keep your card safe and your PIN secret at all times. Your bank or the police will never phone you and ask you to disclose your PIN.

Precautions when using a cash machine:

Cash machines are a very safe way of withdrawing cash and accessing banking services although, unfortunately, they do attract criminal attention. The following advice will help minimise the chances of becoming a victim of such crime.

- Put your personal safety first. Be aware of others around you. If someone is behaving suspiciously or makes you feel uncomfortable choose a different machine. If you spot anything unusual about the cash machine, or there are signs of tampering, do not use the machine and report it to the bank immediately.
- Give other users space to enter their PIN in private. We recommend standing about two metres away from the user in front of you until they have completed their transaction. Some cash machines may have a safety zone marking out this area on the ground around the machine.
- Be alert. If someone is crowding or watching you, cancel the transaction and go to another machine. Do not accept help from seemingly well-meaning strangers and never allow yourself to be distracted.
- Stand close to the cash machine. Always shield the keypad with your spare hand and your body to avoid anyone seeing you enter your PIN.
- Once you have completed a transaction put your money and card away before leaving the cash machine. If the cash machine does not return your card, report its loss immediately to your bank. Tear up or preferably shred your cash machine receipt, mini-statement or balance enquiry when you dispose of them.

Precautions when going abroad with cards:

- Only take the cards you intend to use – store the rest securely at home.
- Some banks suggest that you advise them if you are going to use your card abroad to ensure that any transactions you make are not treated by the card company as unusual spending.
- Make a note of your card companies' emergency contact numbers and keep the information somewhere other than your purse or wallet.

What to do if you are a victim of card fraud in general:

- If you discover that your card has been lost or stolen or that you have been the victim of a fraud tell your card company immediately.
- If someone else uses your card before you tell your card company it has been lost or stolen or before you tell them that someone else knows your PIN, the most you will have to pay, in theory, is £50. In practice the bank or building society will usually refund the full amount lost. But if you are found to have acted fraudulently or without reasonable care, for example, by keeping your PIN written down with your card, you would have to meet all the losses.
- If your card is used fraudulently before you receive it, you will not have to pay for any losses.
- *The Banking Code* offers UK cardholders protection from card fraud losses that is second to none throughout the world. Section 12.12 of *The Banking Code* says that *"unless we* (your card issuer) *can show that you have acted fraudulently or without reasonable care, your liability for the misuse of your card will be limited to £50"*.

Card ID theft – tips to help keep your identity safe:

- Keep personal documents, plastic cards and chequebooks in a safe and secure place. Keep chequebooks and cards separately. Valuable documents include your passport, birth certificate, driving licence, plastic cards, card receipts, financial statements and even utility bills. Without access to this information a criminal will find it very difficult to pretend to be you.
- Don't share personal information unless you are entirely confident you know who you are dealing with. Be particularly cautious if you are cold-called by someone claiming to be from a bank or the police, who then asks you to provide security information. Ask them for their phone number, check that the number is your bank or the police and call them back. Also, be wary of responding to unsolicited e-mails requesting information. Ask for proof of identity or undertake your own checks. Never disclose your PIN to anyone.
- Always check bank statements, and check receipts against your statements carefully. If you find an unfamiliar transaction, contact your card company or bank immediately.
- Carry out an annual credit reference check to make sure that credit hasn't been taken out in your name without you knowing (see page 40 for details).
- Dispose of financial statements, card receipts and other personal documents with care. Rip up or preferably shred any such documents before binning them.
- Be aware that your post is valuable information in the wrong hands. How easy would it be for somebody to intercept your post? If you fail to receive a bank statement, card statement, utility bill or other financial information contact the supplier. If you receive a credit card application and you don't use it, rip it up before throwing it away.

- Guard your cards. Don't let them out of your sight when making a transaction. Report lost and stolen cards, or suspected fraudulent use of your card account, to your bank or card company immediately. Keep a note of your card companies' telephone numbers so that you can easily report lost or stolen cards.
- If you move house make sure you contact your bank and all other organisations to give them your change of address (the Post Office can redirect post on request).

Some warning signs of card ID theft:

- Your regular bank or credit card statements fail to appear.
- You notice that some of your mail is missing.
- Your credit card statement includes charges for items you have not purchased or ordered.
- A debt collection agency contacts you about goods you have not ordered or an account you have never opened.
- You receive a telephone call or letter saying you have been approved or denied credit for accounts you know nothing about.

What to do if you have been a victim of card ID theft:

- Contact your bank or the financial institution concerned and keep a record of all communications.
- Report the incident to the police, especially if it involves stolen identification documents, and ask for a Crime Reference Number, or documentation to record the incident.
- Check with the credit reference agencies detailed below. If applications for credit have been made in your name you can ask to have any incorrect information removed:

  Experian: 0870 241 6212 **www.experian.co.uk**
  Equifax: **www.equifax.co.uk**
  Call Credit: 0870 060 1414 **www.callcredit.co.uk**
- It is useful to obtain a regular copy of your credit report – perhaps annually. A paper copy of your report is available from any of the above agencies for £2.
- Contact CIFAS on 0870 010 2091. They will earmark your name and address so that anyone applying for something using your name will automatically be double-checked.
- If you suspect mail theft contact the Royal Mail Customer Enquiry Number on 08457 740740.

Cheque fraud

42 Types of cheque fraud
43 Common cheque fraud scams
44 Liability for cheque fraud
44 Preventing cheque fraud
45 Consumer advice
47 Retailer advice

What is cheque fraud?

There are three types of cheque fraud in the UK: counterfeit; forged; and fraudulently altered cheque fraud. Last year cheque fraud in the UK amounted to £40.3 million – a 13% decrease from the 2004 total of £46.2million. Previously cheque fraud losses had been on the increase, totalling £36 million in 2002 and £45 million in 2003.

Types of cheque fraud

Counterfeit cheque fraud: £3.2m in 2005
Cheques manufactured or printed on non-bank paper to look exactly like a genuine cheque and drawn by a fraudster on genuine accounts held by the bank.

Forged cheque fraud: £30.9m in 2005
A genuine cheque where part or all of it has been completed by the fraudster. This is the most common type of cheque fraud scam undertaken by organised criminal gangs.

Fraudulently altered cheque fraud: £6.2 million in 2005
A genuine cheque where part or all of it has been altered by a fraudster.

Common cheque fraud scams

A typical cheque fraud involves the criminal buying goods or services and offering to pay for them with a cheque – which has been counterfeited, forged or fraudulently altered. The seller believes the cheque to be genuine, pays it in and waits for it to clear before parting with the goods or services being sold. However, the money can be reclaimed by the bank if the cheque subsequently turns out to be stolen or counterfeit.

Over the past couple of years organised gangs have started to target consumers selling high-value goods such as cars. People selling a high-value item should, therefore, be particularly wary of accepting a cheque or bankers' draft as the gangs typically use stolen or counterfeit cheques and bankers' drafts.

A recent version of this scam involves the fraudster offering a cheque or bankers' draft for significantly more than the price of the goods. The seller is then asked to transfer the amount of the overpayment either directly to them or to a third party after three days when, it is claimed, the cheque will have cleared.

Again, in such a scam, the cheque or draft is not genuine and, whilst banks do all they can to spot and stop such cheques in the clearing system, it may only be after the person selling the goods has received value for the cheque that the genuine cheque owner discovers that money is missing from their account. Consequently, the money paid into the seller's account belongs to someone else and it may be withdrawn from their account. This can sometimes happen several weeks after the money has been paid into the seller's account* by which time the seller has probably transferred the overpayment and even handed over the goods they are selling.

* The innocent victim of cheque fraud may not know that a cheque has been stolen from their chequebook for weeks or sometimes months, particular if they do not check their statement regularly – which is why it can take some time for the money to be reclaimed.

Liability for cheque fraud

Banks will examine each case of cheque fraud on an individual basis but, generally, if you are an innocent victim of cheque fraud who has had a cheque or chequebook stolen and used fraudulently you will be refunded by your bank.

However, if you are a victim of the scam because you have accepted a cheque or bankers' draft that turns out to be fraudulent, and you have parted with either goods or services or, in the case of receiving a cheque or bankers' draft for an inflated amount, you have paid cash back to the buyer, you are unlikely to get the goods back or have the money refunded by your bank.

What is the banking industry doing to prevent cheque fraud?

The banking industry currently focuses its efforts on identifying lost or fraudulent cheques as they pass through the clearing system – before there is a victim. This approach is very successful and in the past year the industry successfully identified more than 90% of all fraudulent cheques as they went through the cheque clearing process. Attempted cheque fraud levels amounted to £631 million in 2004 and £575 million in 2005.

The banking industry is also working to raise public awareness of the issue, urging consumers to remember to be wary of who they accept a cheque or bankers' draft from, especially if it is for a large amount of money.

Consumer advice

Accepting a cheque

- Never accept a cheque, or bankers' draft, from someone unless you absolutely know and trust them. Be especially wary when accepting a high-value cheque – for instance if you are selling a car.
- Be aware that a bankers' draft is not necessarily safe from fraud. If you receive a bankers' draft in payment for goods you must allow time for the draft to clear before releasing the goods. Bankers' drafts can be stolen or altered like any other cheque and if it is altered, stolen or counterfeit it will not be honoured.
- Be aware that, even after the value of the cheque or bankers' draft has been credited to your account, there is a risk that the money could be reclaimed if the cheque or bankers' draft subsequently turns out to be stolen or counterfeit.
- Always consider other types of payment for high-value items – such as an automated phone or internet payment (which takes 48 hours) or a CHAPS payment (a same-day service). There is a charge for a CHAPS payment but it is a guaranteed, irrevocable, same-day value payment. If the buyer is unwilling to pay the relatively small cost involved – or to split it with you – then you need to be on your guard.
- Cheques should be paid into your account as soon as possible to reduce the risk of loss or theft and should always be paid in within six months as older ones may be rejected or returned unpaid.

Writing a cheque

- It will help to prevent fraud if you clearly write the name of the person to whom you are paying the cheque and put extra information about them on the cheque, especially if you are not personally paying a cheque in directly (for example, because you are paying a cheque by post).
- If you are making a cheque payable to a bank or a building society, do not make the cheque payable simply to that organisation. Add further details in the payee line, for example XYZ Bank, re J Jones, account number xxxxxx. (The rules for accepting cheques at banks and building societies are changing from 30 September 2006, in order to safeguard against fraud. After this date, if you try to deposit a cheque in a branch, or by post, made simply to a bank or building society, it is likely to be returned.)
- You should draw a line through unused spaces so unauthorised people cannot add extra numbers or names.
- It is important to minimise fraud by identifying and reporting any misuse of cheques as early as possible. Use chequebook counterfoils to record details of cheques issued and compare them with bank statements. Any discrepancies should be reported to your bank or building society immediately.
- Never presign blank cheques. When writing cheques, be sure to complete all sections, including the payee name, and the amount in both words and figures. To help prevent fraudulent alteration it is good practice to leave as little blank space as possible, if necessary by drawing a line through unused spaces. It is also good practice to include the word 'only' after writing the amount in words.

- If it is necessary to make amendments, these should be made clear by crossing through the error and initialling or signing the correction.
- Always be sure to date cheques – undated cheques are likely to be returned with a request to include a date.
- Personal customers should write cheques in ink – a biro will suffice.

Retailer advice

A cheque is not a guaranteed form of payment. However, the *UK Domestic Cheque Guarantee Card Scheme* gives retailers greater certainty that they will receive payment when accepting cheques. If the Conditions of Use are not met the guarantee is void and cheques could be returned.

The *Scheme* commenced in July 1969 with the objective of creating common, easily identifiable design features to simplify acceptance procedures at the till point. Since 1 October 1990, the common theme has been William Shakespeare and all cards with cheque guarantee functionality depict his image in various ways, e.g. within the cheque guarantee hologram or logo.

The key points of the *Scheme* are:

- One cheque per transaction is guaranteed up to the value limit shown on the accompanying cheque guarantee card.
- Cheques must be dated correctly with the actual date of issue.
- The payee must write the cheque card number on the reverse of the cheque.

- Cheques must be signed by the account holder in the presence of the payee.
- The cheque guarantee card must be valid i.e. it may only be used prior to reaching its expiry date and must not have been altered or defaced.
- When using cheques to obtain cash, customers are limited to one guaranteed cheque per day for this purpose. Frequency-marking pages (usually found at the back of cheque books) are used to keep a record of instances of encashment and to ensure that the one-per-day rule is adhered to.
- The *Scheme* applies to personal cheques and small business cheques only.
- The guarantee applies only to domestic cheques, including those issued in Gibraltar, the Isle of Man and the Channel Islands.

Online fraud

50 Types of online banking fraud
53 Preventing online banking fraud
54 Consumer advice

Online banking fraud

In 2005 total losses from online banking fraud reached £23.2 million – an increase of 90% from the previous year's total of £12.2 million. This fraud is growing from a very small base, which can make losses appear to grow rapidly.

Last year also saw a huge rise in the volume and sophistication of online fraud attempts, which banks and law enforcement have been largely successful in combating. However the vast majority of these scams directly target customers – either attempting to dupe them into disclosing their personal security information or by placing malicious software on inadequately protected computers. It is therefore highly important that customers are aware of the steps they can take to protect themselves. Furthermore, this needs to be seen in context. Online banking fraud losses (£23.2m) are relatively small when compared with plastic card fraud losses (£439.4m).

Types of online banking fraud

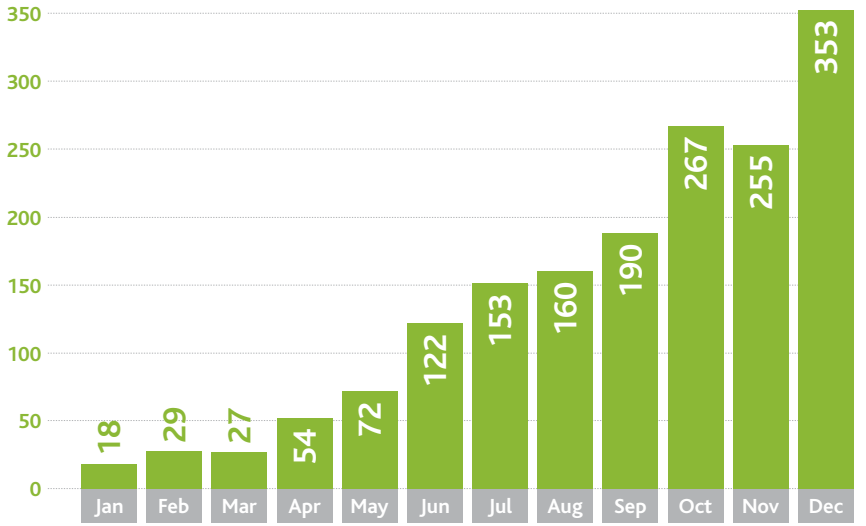
Scams such as phishing and Trojans are responsible for online banking fraud losses in the UK:

Phishing

Phishing is the name given to the practice of sending e-mails at random, purporting to come from a genuine company operating on the Internet, in an attempt to trick customers of that company into disclosing information at a bogus website operated by fraudsters. These e-mails usually claim that it is necessary to 'update' or 'verify' your password and they urge you to click on a link from the e-mail that takes you to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes.

Phishing originated because the banks' own systems have proved incredibly difficult to attack. Criminals have turned their attention to phishing attacks to target individual Internet users in order to gain personal or secret information that can be used online for fraudulent purposes.

Number of phishing incidents* by month in 2005



* In a phishing 'incident' fraudsters set up a website that is a fake version of a genuine bank website, and then send out thousands or even millions of spam e-mails trying to convince people to click on a link that will send them to that fake site. The objective is to fool people into then entering their online banking security information – such as user names, PINs and passwords – onto the fake site.

Trojans

Trojans take their name from the term 'Trojan Horse' and are a type of computer virus that can be installed on your computer without you realising. Trojans are sometimes capable of installing a 'keystroke logger', which captures all of the keystrokes entered into a computer keyboard. Typically the fraudsters will send out e-mails at random to get people to click on a link from the e-mail and visit a malicious website where vulnerabilities in Internet Explorer are exploited to install the Trojan. The e-mails are not normally related to Internet banking and try to dupe people into visiting, or clicking on the link to, the malicious website with a variety of excuses.

Money mules

As most of the fraudsters behind these scams are located overseas and it is not possible to make cross-border transfers out of UK online bank accounts, a money mule or money transfer agent is required to launder the funds obtained as a result of phishing and Trojan scams. After being recruited by the fraudsters, money mules receive funds into their accounts and they then withdraw the money and send it overseas using a wire transfer service, minus a percentage commission payment.

Money mules are recruited by a variety of methods, including spam e-mails, adverts on genuine recruitment websites, approaches to people with their CVs available online, instant messaging and adverts in newspapers.

Although the prospect of making some easy money may appear attractive, any commission payments will be recovered as they are the proceeds of fraud and the money mule may become embroiled in a police investigation. Money mules will be the easiest part of the chain to track down and supplying any information to the fraudsters may also put them at risk from identity fraud.

Preventing online banking fraud

The banking industry works alongside a number of online partners to tackle this type of fraud such as the Serious Organised Crime Agency, overseas law enforcement agencies, technology companies, anti-virus firms and Internet Service Providers.

A number of initiatives are already in place:

- Monitoring of the Internet at industry and bank level to detect and close down phishing-related websites.
- Two-way communication with online partners so security intelligence can be shared and used effectively.
- Development and use of clear and consistent advice for consumers.
- In the longer term, hand-held card readers could be used to create a one-off passcode that is used during the login process to help identify the person as the genuine account holder.

Alongside these initiatives the industry has launched a website at **www.banksafeonline.org.uk** to help online banking users stay safe online. Sections on the site include: types of online banking scams; how to spot these scams; and how to protect yourself from falling victim to these scams. There are also links on the site that enable consumers to report scams to the APACS team of online banking experts and a link that allows consumers to get help and advice from APACS about any industry-wide online banking queries.

Safe Internet usage

- Make sure your computer has up-to-date anti-virus software and a firewall installed. Consider using anti-spyware software. You should also download the latest security updates, known as patches, for your browser from the Internet. If you are a Microsoft Windows user, you are strongly recommended to turn on Automatic Updates. Windows patches can be downloaded from **http://windowsupdate.microsoft.com**
- Make sure your browser is set to the highest level of security notification and monitoring. The safety options are not always activated by default when you install your computer.
- The most popular browsers include Microsoft Internet Explorer, Firefox and Opera. Check that you are using a recent version – you can usually download the latest version from these browsers' websites.
- The banking industry has launched a one-stop consumer and small business advice site at **www.banksafeonline.org.uk** to help Internet users protect themselves from online scams and threats.
- Right click on the security icon to ensure that the website has a valid encryption certificate – the address on this certificate should conform to the address on the address bar. The certificate should ensure the identity of the website and the current day's date should be within the validity dates of the certificate.
- Keep PINs, passwords and personal information safe. Be wary of any unsolicited e-mails requesting your personal financial information, including card details, as these e-mails may not be from a trustworthy source. If in doubt, do not click on any links they contain. Reputable retailers, banks and the police would never ask you to disclose or confirm sensitive personal or security information, including your PIN. If in doubt, phone the organisation first on a number you know to be genuine.

- Check statements from your card company as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. If you find a transaction on your statement that you did not make, contact your card company immediately.
- Ensure you understand the security implications of using file sharing – or peer-to-peer (P2P) applications like Kazaa, Limewire and BitTorrent. P2P applications do have a legitimate use, but sensitive information could be compromised by using them. An individual could unwittingly share any personal information that they have stored within files on their machine. This could include details of bank accounts held, usernames and passwords. As for any file transferred via the Internet, these programs can also introduce security risks such as viruses and Trojans or other malicious code.
- If an unsolicited offer to make money or buy cheap goods online sounds too good to be true, then it probably is!

Contact information

58 Web links
61 Publications
64 Useful contacts
65 Bank and building society contacts
68 Card scheme contacts

Web links

www.apacs.org.uk
APACS is the UK payments association. This site examines its role and different aspects of its work.

www.bankingcode.org.uk
A body that ensures that banks and building societies comply with the standards detailed in *The Banking Code* and *The Business Banking Code*.

www.banksafeonline.org.uk
Assistance for Internet users to help them protect themselves from online scams and threats such as phishing.

www.bba.org.uk
The British Bankers' Association, the principal trade association for banks operating in the UK.

www.bcca.co.uk
The British Cheque Cashers' Association, the trade association of the cheque cashing industry in the UK.

www.callcredit.co.uk
A credit reference agency with a range of information services for businesses and individuals.

www.cardwatch.org.uk
Information about how card fraud takes place in the UK, what is being done to prevent it and how you can help prevent yourself becoming a victim.

www.chipandpin.co.uk
Information, guidance and downloadable materials for businesses and customers about chip and PIN.

www.cifas.org.uk
The UK's fraud prevention service, enables its members to share information on fraudulent activity to help identify and prevent fraud taking place, including on card accounts.

www.consumerdirect.gov.uk
Clear and practical help and advice for consumers in Great Britain.

www.dcpcu.org.uk
Explains how the specialist Dedicated Cheque and Plastic Crime Unit is tackling the prevention of plastic card and cheque crime.

www.equifax.co.uk
A credit reference agency that provides information to businesses, consumers and the public sector.

www.experian.co.uk
A credit reference agency that helps consumers, businesses and the public sector manage their credit information.

www.financial-ombudsman.org.uk
An independent service for resolving disputes between consumers and financial firms.

www.getsafeonline.org
A Government and leading business-sponsored site that provides advice on how to protect your computer and use the Internet with safety.

www.identitytheft.org.uk
How to help protect yourself from identity theft, what to do if it happens to you and suggestions on where to get further help.

www.idfraudpreventiontraining.com
Electronic, tailored, modular training courses for businesses to train their employees on how to check the authenticity of documents used to confirm identity.

www.mastercard.co.uk/securecode
Details of how to sign up and benefit from extra protection when shopping online with a MasterCard.

www.visaeurope.com/verified
Details of how to sign up and benefit from extra protection when shopping online with a Visa card.

Publications

UK Payments 2006
A review of the UK payments industry. Available free of charge from APACS.

UK Payment Statistics 2006
A new annual publication that provides a comprehensive source of UK payment statistics and historical data from 1995 to 2005, with additional forecast data up to and including 2015. Available from APACS at a cost of £750.

The Way We Pay – UK Cash & Cash Machines 2006
Examines the main trends in cash payments, the deployment and usage of cash machines, and other forms of cash acquisition. Available from APACS at a cost of £250.

The Way We Pay – UK Plastic Cards 2006

Details the trends in the use of plastic payment cards in the UK by businesses and individuals. Available from APACS at a cost of £250.

The Way We Pay – UK Automated Payments 2006

Looks at the main trends in the use of direct credits, direct debits, standing orders and CHAPS payments. Available from APACS at a cost of £250.

The Way We Pay – UK Cheques 2006

Examines the main trends in the use of cheques for payment and cash acquisition. Available from APACS at a cost of £250.

Spot & Stop Card Fraud

This pack contains a range of fraud prevention advice for retailers and includes a training video, presentation slides and trainer's notes. This pack is available to download as a PDF from **www.cardwatch.org.uk**. Interactive training is also available on the site.

Counter Attack

A biannual newsletter designed for retail till point staff to increase their fraud prevention awareness. It updates retail staff on ways of preventing card criminals operating in their shops and includes competitions aimed at increasing vigilance.

Spot & Stop Card-not-Present Fraud

A generic training pack developed for managers who train their retail staff to accept card-not-present transactions. The pack gives comprehensive best practice guidelines and examines in detail the solutions available to prevent card-not-present fraud. This pack is available to download as a PDF from **www.cardwatch.org.uk**. Interactive training is also available on the site.

Card Force

A biannual newsletter for police forces across the UK, *Card Force* aims to update police officers on news and issues relating to plastic card crime. It runs stories on plastic card fraud prevention in specific forces, giving case histories and crime fighting tips.

Useful contacts

APACS/Card Watch

020 7711 6259 / 020 7711 6252
press@apacs.org.uk
cardwatch@apacs.org.uk

Sandra Quinn
Director of corporate communications
T: 020 7711 6234 M: 07768 044656
sandra.quinn@apacs.org.uk

Jemma Smith
Head of PR
T: 020 7711 6340 M: 07811 113075
jemma.smith@apacs.org.uk

Mark Bowerman
Communications executive
T: 020 7711 6251 M: 07799 627256
mark.bowerman@apacs.org.uk

Simon Bennett
Press officer
T: 020 7711 6316
simon.bennett@apacs.org.uk

British Bankers' Association

020 7216 8800

DCPCU (media enquiries)

020 7711 6340

Call Credit

0870 060 1414

CIFAS

0870 010 2091

Experian

0870 241 6212

Financial Ombudsman Service

0845 080 1800

Royal Mail Customer Enquiries

08457 740740

Bank and building society contacts

Abbey

Switchboard: 0870 607 6000
Press office: 020 7756 4223
jane.reynolds@abbey.com
www.abbey.com

Alliance & Leicester

Switchboard: 0116 201 1000
Press office: 0116 200 3355
pressoffice@alliance-leicester.co.uk
www.alliance-leicester-group.co.uk

Bank of England

Switchboard: 020 7601 4444
Press office: 020 7601 4411
press@bankofengland.co.uk
www.bankofengland.co.uk

Bank of Scotland (HBOS)

Switchboard: 0870 600 5000
Press office: 0131 243 7077
pressoffice@hbosplc.com

Barclays Bank

Switchboard: 020 7116 1000
Press office: 020 7116 6145
emma.keens@barclays.co.uk

Barclaycard

Switchboard: 01604 234 234
Press office: 01604 251 229
pressoffice@barclaycard.co.uk
www.barclaycard.co.uk

Capital One

Switchboard: 0115 843 3300
Press office: 0115 843 3174
richard.holmes@capitalone.com
www.capitalone.co.uk

Citigroup

Switchboard: 020 7986 4000
Press office: 020 7986 5602
jeremy.hughes@citigroup.com
www.citigroup.com

Clydesdale Bank
Switchboard: 0141 248 7070
Press office: 0141 242 4357
yolande.stratford@eu.nabgroup.com
www.cbonline.co.uk

Co-operative Bank
Switchboard: 0161 832 3456
Press office: 0161 829 5397
david.smith@cfs.co.uk
www.co-operativebank.co.uk

Coutts Group
Switchboard: 020 7753 1000
Press office: 020 7957 2427
nick.gill@coutts.com
www.coutts.com

Egg
Switchboard: 020 7526 2500
Press office: 020 7526 2600
prteam@egg.com
www.egg.com

GE Capital
Press office: 020 7853 1987
stewart.macphail@ge.com
www.gecapital.com

Halifax (HBOS)
Switchboard: 0870 600 5000
Press office: 01422 333 253
markhemingway@halifax.co.uk
www.hbosplc.com

HFC Bank
Switchboard: 01344 890 000
Press office: 01344 892559
patrick.long@hfcbank.co.uk
www.hfcbank.co.uk

HSBC
Switchboard: 020 7991 8888
Press office: 020 7991 0641
pressoffice@hsbc.com
www.hsbc.com

Lloyds TSB Bank
Switchboard: 020 7626 1500
Press office: 020 7356 2493
mary.walsh@lloydstsb.co.uk
www.lloydstsb.com

MBNA Europe Bank
Switchboard: 01244 672 000
Press office: 01244 574404
john.greaves@mbna.com
www.mbna.com

Morgan Stanley
Switchboard: 020 7425 8000
Press office: 020 7425 8005
euart.glendinning@morganstanley.com
www.morganstanley.com

National Australia Bank
Switchboard: 020 7710 2100
Press office: 020 7710 2435
ken.pipe@eu.nabgroup.com
www.national.com.au

Nationwide
Switchboard: 01793 656000
Press office: 01793 655 198
pressoffice@nationwide.co.uk
www.nationwide.co.uk

Natwest Group
Switchboard: 020 7427 8000
Retail bank press office: 020 7672 1931
ronan.kelleher@natwest.com
www.natwest.com

Northern Rock
Switchboard: 0191 285 7191
Press office: 0191 279 4676
press.office@northernrock.co.uk
www.northernrock.co.uk

The Royal Bank of Scotland
Switchboard: 0131 556 8555
Retail bank press office: 020 7672 5086
laura.mottram@rbs.co.uk
www.rbs.co.uk

Standard Chartered
Switchboard: 020 7280 7500
Press office: 020 7280 7163
sean.farrell@uk.standardchartered.com
www.ukstandardchartered.com

Woolwich
Switchboard: 020 8298 5000
Retail press office: 020 7116 6229
emma.austin@barclays.com
www.woolwich.co.uk

Card scheme contacts

VISA International
Switchboard: 020 7937 8111
Press office: 020 7937 8111
europeanmedia@visa.com
www.visa.com

MasterCard International/Maestro
Press office: 0870 990 5403
mastercardpressoffice@webershandwick.com
www.mastercardintl.com
www.maestrocard.com

American Express
Switchboard: 01273 693 555
Press office: 020 7976 4677
paconsultant@aexp.com
www.americanexpress.com

Diners Club
Switchboard: 0870 190 0011
Press enquiries: 0870 190 0011

APACS is the UK trade association for payments. It provides the forum for the UK's financial institutions to come together on non-competitive issues, to develop banking systems for the future and to provide innovation and developments in payments. It is also the banking industry voice on payments issues such as plastic cards, payment fraud, cheques, electronic payments and cash.

For further information about Card Watch visit www.cardwatch.org.uk or e-mail cardwatch@apacs.org.uk.
For more copies of this booklet e-mail corpcomms@apacs.org.uk

APACS
the UK payments association

Mercury House, Triton Court, 14 Finsbury Square, London, EC2A 1LQ
www.apacs.org.uk