

2005 **Card Fraud** The Facts

The definitive guide for the media on plastic card fraud and measures to prevent it



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.

At the forefront of reducing card fraud is APACS’ Plastic Fraud Prevention Forum (PFPF), which includes representatives from all the UK’s major card issuers and the international card schemes, including Visa and MasterCard. It develops and implements strategies to prevent card fraud and since the early 1990s has led Card Watch, the public awareness campaign.

“Although plastic card fraud losses increased in 2004 this was by no means due to a drop-off in our efforts to stop those responsible. On the contrary, the organised criminal groups responsible for recent increases in card fraud have realised that the UK’s implementation of chip and PIN will dramatically curtail their ability to commit these types of crime and, therefore, they have been increasing their activity accordingly.

The outstanding efforts by all involved in the roll-out of chip and PIN and the establishment of the specialist police squad, the Dedicated Cheque and Plastic Crime Unit, as a permanent unit are two highlights from last year. Both are developments that will play a major part in significantly reducing predicted levels of card fraud.

Our continuing drive to tackle card fraud in all its guises will go on unabated. Our work with the retail industry, law enforcement and the Home Office will continue on both short-term and long-term solutions in the battle against those responsible for card fraud.”

Jon Berrill – Chairman of APACS’ Plastic Fraud Prevention Forum

Types of Fraud

2004 plastic card fraud on UK-issued cards

6	Card-not-present	£150.8m	+24% from 2003
8	Counterfeit	£129.7m	+17%
10	Lost and stolen	£114.4m	+2%
12	Mail non-receipt	£72.9m	+62%
14	Identity theft	£36.9m	+22%
	Total:	£504.8m	+20%*
	Contained within this total:		
16	Cash machine fraud	£74.6m	+81%
18	Fraud abroad	£92.5m	-11%
20	Internet fraud	£117.0m	

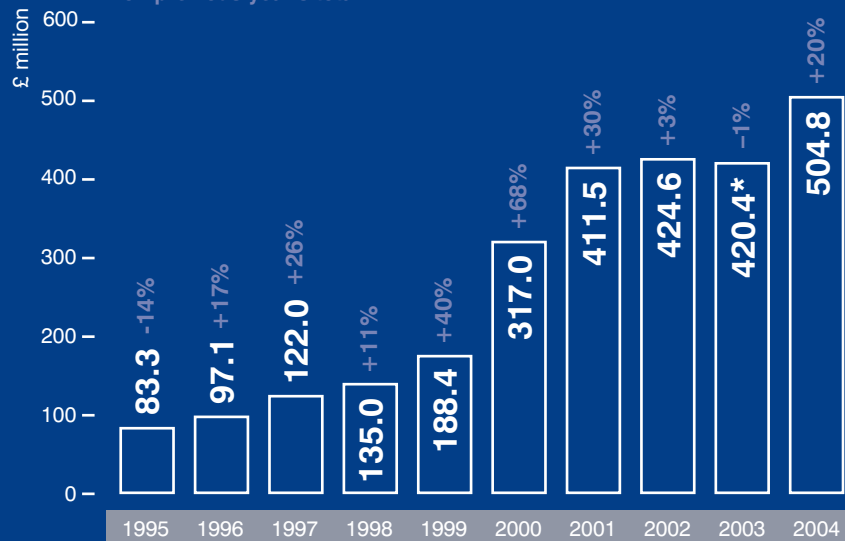
Why has card fraud gone up?

Plastic card fraud losses on UK-issued cards rose by 20 per cent in 2004 because the organised criminal groups responsible have increased their illegal activities before the full security benefits of chip and PIN are realised. From 2005 onwards we expect to see a decline in domestic counterfeit and lost and stolen card fraud due to the implementation of chip and PIN.

*Note: Plastic card fraud losses for 2003 have been adjusted to include losses that were reported after original publication of the 2003 fraud figures.

Plastic card fraud losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



*Figure adjusted from that detailed in *Card Fraud the Facts 2004*

Annual plastic card fraud losses on UK-issued cards 1995 – 2004

All figures in £millions

Year	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Type of fraud										
Card-not-present	4.6	6.5	10.0	13.6	29.3	72.9	95.7	110.1	122.1	150.8
Counterfeit	7.7	13.3	20.3	26.8	50.3	107.1	160.4	148.5	110.6	129.7
Lost/Stolen	60.1	60.0	66.2	65.8	79.7	101.9	114.0	108.3	112.4	114.4
Mail non-receipt	9.1	10.0	12.5	12.0	14.6	17.7	26.8	37.1	45.1	72.9
Identity theft	1.8	7.2	13.1	16.8	14.4	17.4	14.6	20.6	30.2	36.9
UK total	62.1	71.6	92.8	100.1	134.1	213.4	273.0	294.4	316.3	412.3
Fraud abroad	21.2	25.4	29.2	34.9	54.2	103.5	138.4	130.2	104.1	92.5
Total	83.3	97.1	122.0	135.0	188.4	317.0	411.5	424.6	420.4	504.8

>> Card-not-present fraud £150.8m in 2004

Fraud on phone, Internet, mail order or fax transactions

Card-not-present (CNP) fraud is perpetrated through the theft of card details for use in non face-to-face transactions and is now the largest type of card fraud in the UK.

The problem in countering this type of fraud lies in the fact that neither the card nor the cardholder is present at a till point in a shop. This means that:

- CNP businesses are unable to check the physical security features of the card to determine if it is genuine
- Without a signature or a PIN it is not easy to confirm that the customer is the genuine cardholder
- Card issuers 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 CNP businesses protect themselves from card-not-present fraud (see page 26).

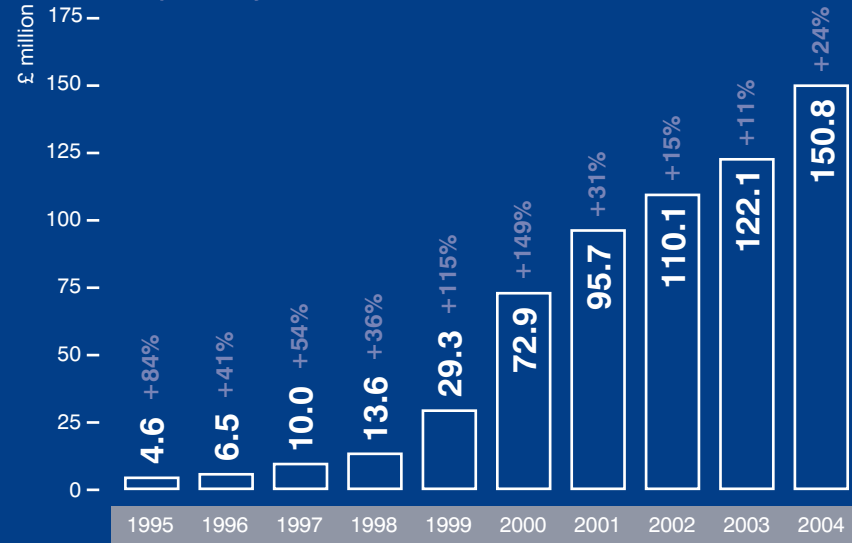
What is card-not-present fraud?

This crime most commonly involves the theft of genuine card details that are then used to make a purchase through a remote channel such as the phone, Internet, mail order or fax. The legitimate cardholder may not be aware of this fraud until they check their statement.

- >> **Cardholders should keep cards safe and in sight at all times and discard receipts carefully – shred or rip them up first – and always check statements for unfamiliar transactions.**

Card-not-present fraud losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



>> Counterfeit card fraud £129.7m in 2004

Counterfeit card fraud increased by 17 per cent to £129.7 million in 2004 – the main reason being an increased effort by organised criminals to commit this type of fraud before chip and PIN prevents them.

Once we reach the situation where – to all intents and purposes – all face-to-face card purchases are made with chip and PIN, we expect to see significant reductions in counterfeit card fraud losses.

What is counterfeit card fraud?

A counterfeit, cloned or skimmed card is one that has been printed, embossed or encoded without permission from the card company, or one that has been validly issued and then altered or recoded.

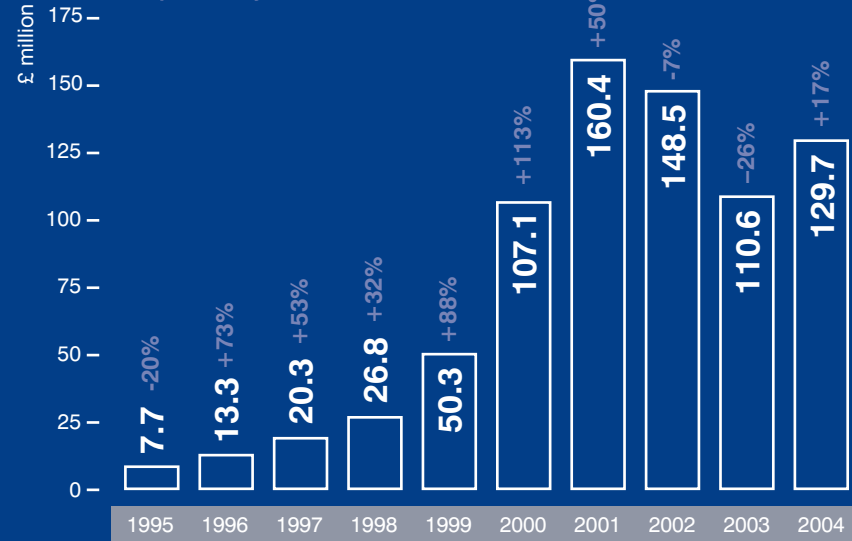
Most cases of counterfeit fraud involve skimming, a process where the genuine data on a card's magnetic stripe is electronically copied onto another, without the legitimate cardholder's knowledge.

Skimming often occurs at retail outlets – particularly bars, restaurants and petrol stations – where a corrupt employee skims a customer's card before handing it back, then sells the information on higher up the criminal ladder where counterfeit 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 (see page 16).

>> **Cardholders should keep their cards in sight at all times when making a transaction and always check their statements for transactions they did not make.**

Counterfeit fraud losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



>> Lost and stolen card fraud £114.4m in 2004

Fraud on lost and stolen cards amounted to £114.4 million in 2004. This type of card fraud has remained fairly static for the past five years, but a decrease is expected once chip and PIN is fully rolled out in the UK.

The banking industry has a number of initiatives in place to tackle lost and stolen card fraud:

- Chip and PIN will significantly reduce this type of fraud as criminals will not be able to use a stolen card in a face-to-face transaction, as they will not know the PIN.
- A retailer education programme, run by APACS since 2001, provides help for shop staff on how to detect stolen and counterfeit cards at the point-of-sale. An online version of this retailer training programme is also available.
- Intelligent computer systems that can track customer accounts for unusual spending patterns.
- An Industry Hot Card File enables retailers to electronically check whether a card has been reported lost or stolen.

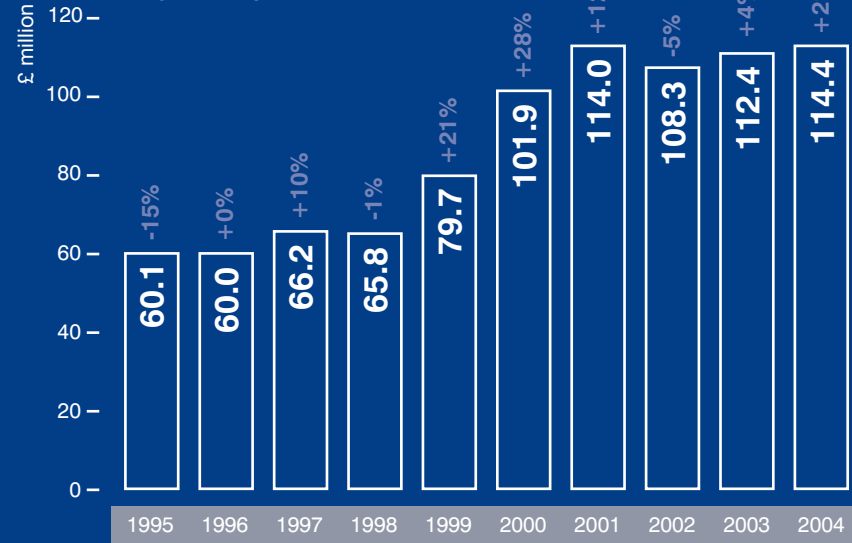
What is lost and stolen card fraud?

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 before the cardholder has reported the loss.

- >> **Cardholders should report a missing card to their issuing bank immediately to enable the card to be blocked.**

Lost and stolen fraud losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



>> Mail non-receipt fraud £72.9m in 2004

This type of fraud increased 62 per cent to £72.9m in 2004, representing just over 14 per cent of total fraud losses. The main reason behind this large increase is the fact that the rollout of chip and PIN resulted in more cards than ever before being issued last year. In August 2004, for instance, 8.7 million cards were issued – 281,000 per day. This meant that the opportunity for this type of fraud to take place was increased. However, the cards and PINs are sent out separately making it harder for criminals to obtain both and as chip and PIN becomes more widespread the number of shops where a criminal can use a stolen card without a PIN will decrease.

The banking industry is working with all the organisations it uses to deliver its cards to monitor card losses, identify fraud hot spots and take preventative action – for example asking cardholders to collect cards from a branch in person, requiring cardholders to phone their card companies before cards can be used, or using more secure couriers.

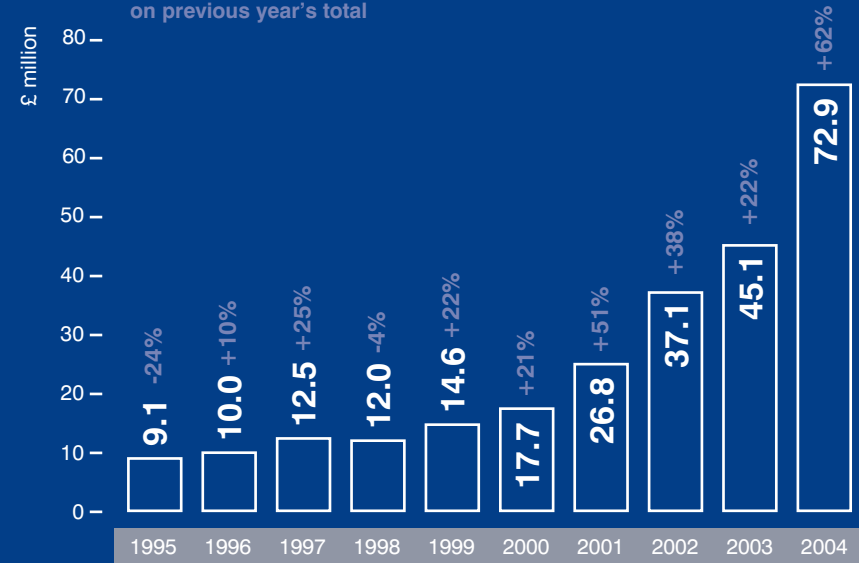
What is mail non-receipt fraud?

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.

>> **Contact your issuing bank if you are concerned about the safe delivery of a plastic card.**

Mail non-receipt fraud losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



>> Identity theft £36.9m in 2004

Although identity theft currently accounts for seven per cent of overall card fraud, the UK banking industry is preparing for a possible rise once chip and PIN makes its impact, as criminals will look for different ways to perpetrate fraud. It is estimated that more than 100,000 people are affected by all types of identity theft in the UK each year, costing the British economy over £1.3 billion annually.

What is identity theft on a card account?

ID theft on cards occurs when a criminal uses fraudulently obtained personal information to open or access card accounts in someone else's name. There are two types:

Application fraud (£13.1m in 2004)

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. This type of fraud decreased by 14 per cent year-on-year.

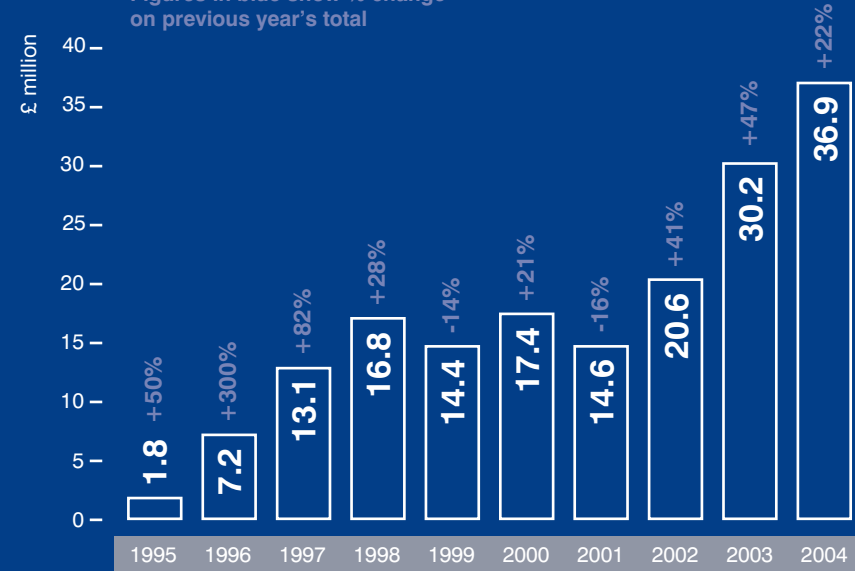
Account take-over (£23.8m in 2004)

By obtaining key personal information, criminals are able to take over the running of a genuine cardholder's account. By pretending to be the genuine cardholder, the criminal will try to deceive the bank or card company and arrange for payments to be taken from the account. The criminal will also instruct the bank to change various details of the account, such as the address, and then ask for new cards and chequebooks to be issued. This type of fraud increased by 60 per cent in 2004.

>> **Discard personal documentation with care – shred it if possible.**

Identity theft losses on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



>> Where does card fraud take place?

In 2004 most plastic card fraud on UK-issued cards was committed via face-to-face transactions in a shop in the UK: £218.8m in 2004. Other locations for fraud include:

>> Cash machine fraud £74.6m in 2004

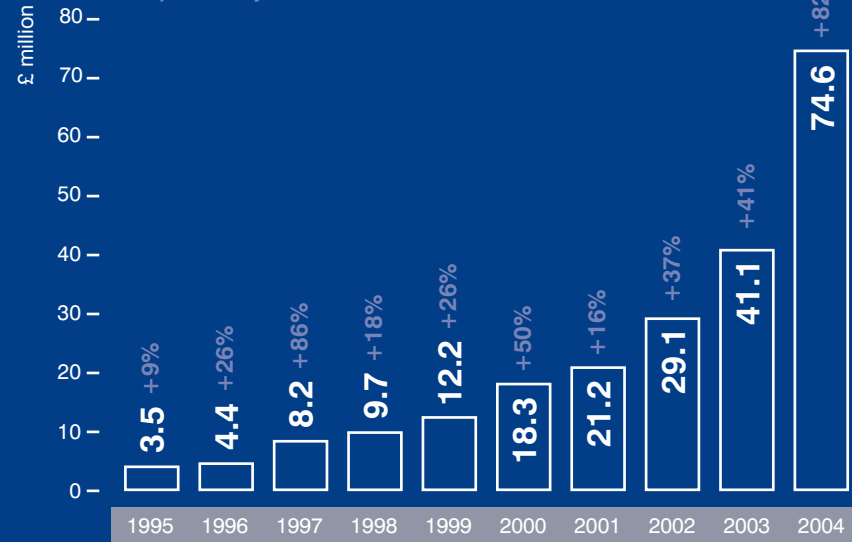
Cash machine fraud is not a type of fraud but describes the location where it occurs. Although fraud at cash machines in the UK has increased significantly in the last three years, it accounts for less than 15 per cent of total plastic card fraud losses.

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

- Skimming at cash machines – this is now the most common way that cash machine fraud takes place. 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. This enables the criminal to produce a counterfeit card and withdraw money at a cash machine using the legitimate 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.
- 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 1995 – 2004

Figures in blue show % change on previous year's total



A number of initiatives are now in place or being developed to counter all these types of fraud including:

- the introduction of chip and PIN, which will effectively combat the use of skimmed cards in cash machines
- making cash machines tamper-proof
- installing CCTV and siting 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)

>> Use your spare hand to shield the keypad when you enter your PIN

>> Fraud abroad (£92.5m in 2004)

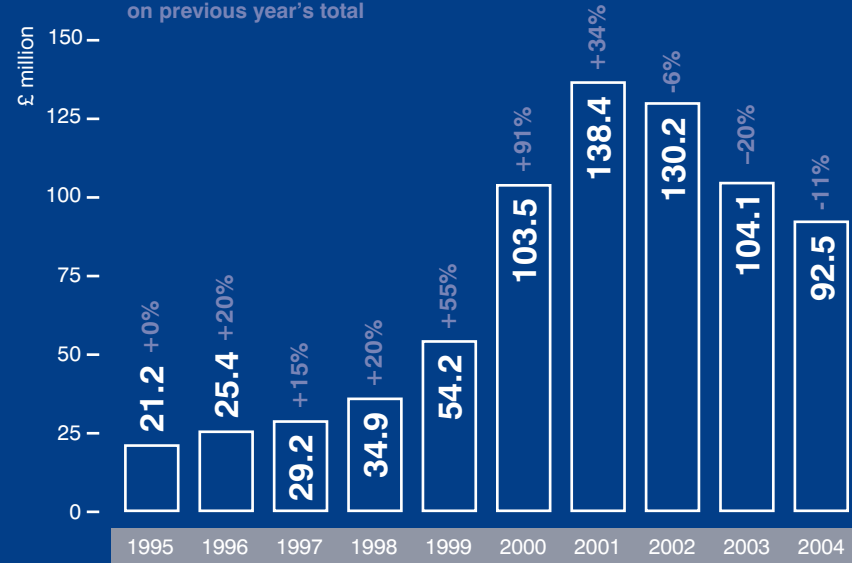
Just under a fifth of fraud (18 per cent) on UK cards occurs abroad. Since 2001, fraud abroad has declined by 33 per cent, a figure all the more impressive as total card fraud has increased by 23 per cent during the same period. The main reasons for this reduction are:

- card companies' increased use of intelligent fraud-detection systems (see page 28)
- the work of the DCPCU, which has cracked several counterfeiting groups with international links (see page 24)

Just under half (48 per cent) of fraud abroad took place in three countries. The USA accounted for 18 per cent (£16.4m) of losses on UK cards used abroad; France 17 per cent (£15.8m); and Spain 13 per cent (£12.3). These figures are not just the

Fraud committed abroad on UK-issued cards 1995 – 2004

Figures in blue show % change on previous year's total



result of British holidaymakers having their cards stolen in these countries. Most of the fraud on UK cards in these countries is a result of fraudsters using card details taken from people still in the UK, using means such as skimming.

» **Fraud on the Internet / e-commerce fraud** estimated at £117.0m in 2004

Card-not-present fraud losses on UK-issued cards totalled £150.8 million in 2004. The amount of this fraud that took place over the Internet is estimated at £117 million - 78 per cent of total 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 or bin-raiding. 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 email 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.

Late 2003 was the first time that phishing came to prominence in the UK. Fraud losses caused by phishing – which involves criminals trying to trick people into revealing their personal financial information through bogus emails – totalled £12 million in 2004.

Preventing Fraud

- 22 **Chip and PIN**
- 24 **Dedicated Cheque and Plastic Crime Unit**
- 25 **Fraud Intelligence Bureau**
- 25 **Helping retailers fight fraud**
- 26 **Systems to reduce CNP fraud**
- 28 **Intelligent fraud-detection systems**
- 28 **Identity theft prevention**
- 29 **Preventing fraud on the Internet**
- 30 **CIFAS**
- 31 **Lower floor limits**
- 31 **Industry Hot Card File**

>> Chip and PIN

The more secure way to pay by plastic

Most UK cardholders now have chip and PIN cards and shops up and down the country have upgraded to chip and PIN. Chip and PIN is the biggest change to the way we pay since decimalisation and is part of a global programme to tackle soaring levels of 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 current magnetic stripe making chip and PIN cards much harder to counterfeit. The second is the four-digit PIN, which is used to prove you are the genuine cardholder. It is a much safer way to prove you are the genuine cardholder as it cannot be forged in the way that a signature can.

National roll-out

By the end of February 2005, 36 million of the UK's 42 million cardholders had received at least one chip and PIN card and more than 700,000 out of the country's 860,000 point-of-sale terminals had been upgraded to chip and PIN. At that time about 50 shop transactions per second were made with chip and PIN cards – about 25 million a week – and this figure is growing all the time.

The majority of shop transactions are now made with chip and PIN and the key challenge for 2005 is to complete the chip and PIN rollout in the UK so that – to all intents and purposes – all face-to-face card purchases are made using chip and PIN.

Chip and PIN for people with a disability

Chip and PIN is good news for customers with disabilities as many customers who have found signature difficult to use find PIN much more convenient. Cardholders with a disability who think they may have difficulty with chip and PIN should talk to their card company who will discuss the best solution for them.

The views and needs of disabled cardholders have, and continue to be, taken into account during the planning for and the rollout of chip and PIN. This has included regular forums, meetings, research and close collaboration with local and national disability groups including the RNIB and the Disability Rights Commission.

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 will be the first major market to complete its rollout. 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 only provide a costly short to medium-term solution. With the introduction of PINs, the banking and retailer industries are shifting the responsibility of identifying the cardholder 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 special police unit targeting organised card criminals

The two-year pilot of the DCPCU concluded in April 2004. It was then established as a permanent unit and is, uniquely, fully funded by the banking industry. During the eight months following the pilot, the DCPCU arrested 102 suspects and achieved £7.7 million of potential savings to the banking industry through the recovery of more than 4,800 counterfeit cards and compromised card numbers.

Since April 2004 the Unit's remit has been broadened beyond counterfeit fraud to encompass other categories of serious and organised cheque and plastic crime. The Unit is jointly resourced, with APACS and its members providing fraud investigators and administrators who work alongside officers from the City 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, particularly skimming. It has helped identify several major counterfeiting rings run by organised criminals. In 2004 the FIB tracked a sharp rise in skimming attacks at cash machines, and a continuation of those at retail outlets.

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.

>> Helping retailers fight fraud

Training and rewarding shop staff for stopping fraud

Tactical programmes to reduce card fraud losses are a key part of the industry's work with fraud-prone card-accepting businesses. The aim of these programmes is to create a greater awareness amongst shop staff and maximise the number of fraudulent cards that they capture.

Initiatives include:

- Incentivising staff through increased and supplemented rewards – the banking industry paid out £16 million to retail staff who retained fraudulent cards in 2004
- Regular updates to relevant businesses on fraud losses at store level
- The provision of ultraviolet lamps to help identify counterfeit cards

More than 4,000 lost, stolen and counterfeit cards were captured in 2004 as a result of this training, with estimated savings to retailers and the banking industry exceeding £2 million.

Underlying these initiatives is APACS' *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 is available at www.cardwatch.org.uk.

Spot & Stop Card Fraud is part of a wider, on-going retailer education programme that incorporates a range of free publications (see page 54).

>> Systems to reduce card-not-present fraud

Helping businesses fight CNP fraud

Although card-not-present fraud – via the phone, Internet, mail order and fax – 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 five-pronged strategy is in place to counter this type of fraud.

In the short term:

- 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 a

special security code on the card. These extra data checks provide additional information to help businesses assess potential fraud risks and decide whether to proceed with the transaction.

- Visa and MasterCard have each introduced secure payment systems (*Verified by Visa* and *MasterCard SecureCode*) for safer online transactions. (www.visaeurope.com/verified and www.mastercard.com/securecd)
- Retailers are encouraged to make use of various card-not-present fraud prevention tools, such as intelligent fraud detection software, available from third-party providers
- Promotion of the APACS publication – *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.
- In the longer term, chip and PIN cards may help prevent CNP fraud through the development of pocket-sized card-accepting devices that can be used with phones and computers by generating a dynamic password for use solely in the CNP environment (referred to as token-based authentication).

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.

>> 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 in the UK, and internationally as well, with considerable success.

>> Identity theft prevention

Cross-industry co-operation to fight ID theft

As chip and PIN begins to reduce certain types of fraud it is likely that organised criminal gangs may turn their attention to areas such as identity theft.

Over two years ago a multi-sector working group, involving APACS, British Bankers' Association, CIFAS, key government departments and law enforcement bodies, was set up to tackle this type of fraud.

This has resulted in a number of initiatives:

- APACS has published *Identity Fraud – the UK Manual* in conjunction with CIFAS and the Finance & Leasing Association with the support of the Home Office. The

Manual and its supporting material, including a training programme and best practice guidelines, explain how businesses and organisations can best protect themselves and their customers.

- An online training site has been launched at www.idfraudpreventiontraining.com by APACS, the British Bankers' Association and CIFAS, with Home Office backing. It provides best practice guidelines for businesses that could be targeted by identity fraudsters and features an interactive e-training section to improve the understanding of employees who need to check the identity of customers on a day-to-day basis.
- A Home Office Identity Fraud Steering Committee, consisting of senior representatives from the public and private sectors, includes APACS, and brings together all those with an interest in reducing identity fraud in the UK.
- www.identitytheft.org.uk – a consumer-focused website launched by the Home Office. It advises the public how to best protect themselves from identity theft and has advice for victims.

>> Preventing fraud on the Internet

Secure methods to prevent online fraud

Most Internet fraud involves using card details fraudulently obtained in the real world – such as corrupt employees in pubs and restaurants copying the details when cards leave the cardholders' sight or from criminals stealing carelessly discarded financial information. Cardholders can help prevent this happening by being aware that cards and card details are valuable and by not letting them out of their sight. A comprehensive list of what cardholders can do to avoid becoming a victim of Internet fraud can be found on page 35.

In addition, 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* are personal password-protected services that enable 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.

The banking industry has also launched www.banksafeonline.org.uk for consumers and small businesses, to help Internet users protect themselves from online scams and threats such as phishing.

For both Internet and the more traditional forms of card-not-present fraud the possible roll-out of token-based authentication (see page 27) could help to reduce losses, primarily in the UK but also potentially across Europe.

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

>> **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.

>> **Lower floor limits**

Online checks to ensure cards have not been reported as being used fraudulently

Most retail outlets and card-accepting businesses have a floor limit – an amount above which they will seek authorisation from the card issuer before completing a transaction. Around 70-80 per cent of transactions are authorised.

>> **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 440,000 cases of attempted fraud were prevented by this system in 2004.

The IHCF is also being used successfully at tollbooths in France to combat the use of stolen UK cards at road tolls.

Cardholder Advice

- 34 General advice
- 34 Safe phone shopping
- 35 Safe Internet usage
- 37 Choosing a PIN
- 38 Keeping a PIN secret
- 38 Using a cash machine
- 40 Going abroad with cards
- 40 If you are a victim of card fraud
- 41 Keeping your ID safe
- 42 Warning signs of ID theft
- 43 If you are a victim of ID theft

>> General advice

- Don't let your cards or card details out of your sight when making a transaction.
- Don't carelessly discard receipts from card transactions. Tear up, or preferably shred, any documents that contain information relating to your financial affairs.
- Check receipts against statements carefully. If you find an unfamiliar transaction, contact your card issuer immediately.
- Never write down your PIN and never disclose it to anyone, even if they claim to be from your bank or the police.
- Be wary of anyone trying to watch you enter your PIN, especially at a cash machine. Do not allow yourself to be distracted and shield the keypad with your spare hand.
- Report lost or stolen cards or suspected fraudulent use of your card account 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 may 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 – including over the phone. Your bank or the police will never ask you to disclose your PIN.
- Always ask the retailer to confirm the full price to be charged to your card, including any booking fees, delivery charges etc. Make a note of this at the time.
- 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.
- Always check the statements from your bank or card company carefully as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. Contact your card company if the matter is not resolved to your satisfaction.
- If you find any transactions on your statement that you are certain you did not make, contact your card company immediately. You may be asked to sign a disclaimer, confirming that you did not undertake the transaction.

>> Safe Internet usage

- Make sure your computer has up-to-date anti-virus software and a firewall installed. You should also download the latest security updates, known as patches, for your browser from the Internet. Internet Explorer users can download them 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.
- Only shop at secure websites – ensure that the security icon, the locked padlock or unbroken key symbol, is showing in the bottom right of your browser window before sending your card details. The beginning of the retailer's Internet address will 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 or that carry the TrustUK logo.
- Click on the security icon to ensure that the retailer 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 unsolicited e-mails requesting your personal financial information, including card details, as these e-mails may not be from a trustworthy source. 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.
- 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). Make a note of any 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 this information will help your card company take up your case if required.

- 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.
- 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.
- If you regularly make transactions over the Internet consider opening a separate credit card account specifically for these transactions.
- 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.
- If an unsolicited offer to make money or buy cheap goods online sounds too good to be true, then it probably is!

Further information about e-shopping is available by visiting the Department of Trade and Industry's Consumer Gateway site at www.consumerdirect.gov.uk.

>> Advice when choosing your 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, whichever is easiest to remember – 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 your football team last won the FA Cup or the number of letters in a four-word phrase that you can easily remember (e.g. 'Card Fraud the Facts' would equate to 4535). Rather than remembering a PIN digit-by-digit, learn the pattern that you need to trace on the keypad with your fingers.

>> Keeping your PIN a secret

- Don't allow anyone else to use your card, PIN or other security information.
- When entering your PIN in a shop, restaurant or cash machine use your spare hand or your body to shield the number from any prying eyes.
- 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.
- Never write down or record your PIN or other security information.
- 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.

Choosing a cash machine

- 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.

Using a cash machine

- 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.

Leaving a cash machine

- 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 bank or 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 the cardholder is found to have acted fraudulently or without reasonable care, for example, by keeping their PIN written down with their card, they would have to meet all the losses.
- If your card is used fraudulently but you still have the card in your possession you will not be liable to pay for any losses. You may still have your card in your possession if you are a victim of card-not-present fraud or if the magnetic stripe on your card has been counterfeited.

- 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.

>> ID fraud – 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 whom you are dealing with. Be particularly cautious if you are cold-called by someone claiming to be from a bank or the police. Your bank would only ever ask for specific characters within your password, not the whole password. Ask them for their phone number, check it 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.
- 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 building society immediately. Keep a note of your card issuers' 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 ID theft and fraud

- 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 ID fraud

- Contact your bank or financial institution concerned and keep a record of all communication.
- 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: 0870 514 3700 www.equifax.co.uk
Call Credit: 0870 060 1414 www.callcredit.co.uk
- It can be useful to get a copy of your credit report. This is available from all the above agencies for a small fee (typically £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.**

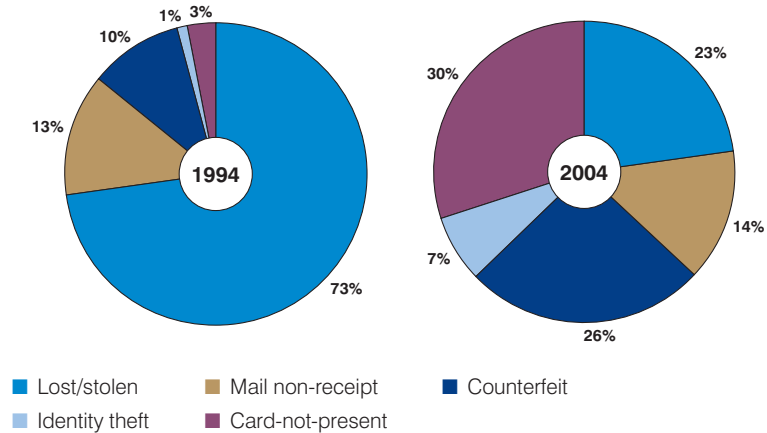
Facts and Figures

as of Dec 2004

- 46 Overview
- 47 Regional hot spots
- 48 Plastic card facts
- 49 Cash machine facts
- 51 Card fraud facts
- 52 Web links
- 54 Publications
- 56 Useful contacts

>> Overview

To put plastic card fraud losses into context it should be noted that card usage and the number of cards issued continues to rise in the UK. However, plastic card fraud losses against total turnover – at 0.141 per cent – are significantly less than the 1991 peak level of 0.33 per cent. This fraud-to-turnover ratio rose slightly (5 per cent) from 0.135 per cent in 2003.



Fraud in the UK in 2004 on UK-issued cards

Regional hot spots

Region	£mn
South East (Inc Greater London)	206.8
North West	32.1
West Midlands	21.5
Yorkshire and Humberside	20.2
East Midlands	19.8
Scotland	14.3
South West	11.0
East Anglia	7.7
North East	6.8
Wales	6.3
Northern Ireland	1.0
Greater London (Inc Inner London)	152.3
Inner London	108.9

>> Plastic card facts as of 31 December 2004

- Credit cards were first issued in the UK in 1966 and debit cards in 1987.
- There are more than 166 million plastic cards (160 million in 2003) in issue in the UK:
 - 66.8 million debit cards (62.9 million in 2003)
 - 69.9 million credit cards (66.8 million in 2003)
 - 24.8 million stand-alone cash machine cards (24.9 million in 2003)
 - 4.4 million charge cards (4.4 million in 2003)
 - 0.8 million cheque guarantee cards (1.6 million in 2003)
- Over 8.3 billion transactions were made on UK cards in 2004
- The total value of all transactions reached £464 billion in 2004
- Debit cards were used 3.7 billion times for purchases with a value totalling over £150 billion in 2004
- Credit and charge cards were used 1.9 billion times for purchases with a value of £123 billion in 2004
- The average purchase value on a UK-issued credit card in the UK is around £58
- The average purchase value on a UK-issued debit card in the UK is £41

>> Cash machine facts

- The first cash machines were introduced in 1967. The early machines dispensed fixed amounts of cash in exchange for tokens. It was only from 1972 that magnetic stripe cards were introduced to enable cash withdrawal.
- Until 1999 all cash machines in the UK were owned and operated by banks and building societies. From 1999, independent cash machine deployers have entered the market and installed cash machines in retail locations such as newsagents and pubs.
- There are 54,412 cash machines in the UK – up from 46,461 in 2003
- In 2004 95.1% of all cash machine withdrawals and 96.6% of all cash withdrawn were from cash machines owned by banks and building societies
- In 2004 there were 2.53 billion cash withdrawals from cash machines in the UK – an average of 80 per second
- The total value withdrawn from cash machines in the UK in 2004 was £161.3 billion – an average of £5,114 per second
- The average cash withdrawal at a bank or building society-owned cash machine is £65 and £45 at an independently-owned machine
- 32.9 million adults in the UK are regular cash machine users

Number of cash machines in the UK

Year	Banks and building societies	Independent deployers	Total
1995	20,933	0	20,933
1996	22,121	0	22,121
1997	23,193	0	23,193
1998	24,574	0	24,574
1999	27,379	0	27,379
2000	29,102	3,898	33,000
2001	30,072	6,594	36,666
2002	31,317	9,508	40,825
2003	32,025	14,436	46,461
2004	32,729	21,683	54,412

>> Plastic card fraud facts

- £504.8 million of card fraud took place on UK-issued cards in 2004. This was split up into:
 - **Card-not-present** £150.8 million
 - **Counterfeit** £129.7 million
 - **Lost and stolen** £114.4 million
 - **Mail non-receipt** £72.9 million
 - **Identity theft** £36.9 million
- Almost £1.4 million worth of card fraud occurs on UK-issued plastic cards every day
- A fraudulent card transaction takes place every seven seconds
- Just over 53 per cent of all fraudulent card use in the UK takes place at the retail point-of-sale
- In 2004 the average loss per fraudulent case was £696
- In 2004 the average value of a fraudulent transaction was £117
- If chip and PIN was not put into action, forecasts estimate that UK card fraud losses would be in the region of £800 million by the end of 2005 and £1 billion per year by the end of the decade

>> Web links

www.apacs.org.uk

APACS is the UK payments association. This site explains its role and different aspects of its work

www.banksafeonline.org.uk

assistance for Internet users to help them protect themselves from online scams and threats such as phishing

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

a fraud prevention service enabling 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.dcpku.org.uk

explains how the special police 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.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.com/securecd

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



Spot & Stop Card Fraud retailer training pack

This pack contains a range of fraud prevention advice for retailers and includes presentation slides, trainer's notes and a four-step fraud prevention guide. This pack is available to download as a PDF from www.cardwatch.org.uk.



Counter Attack

A biannual newsletter designed for retail point-of-sale 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.



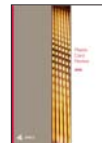
Spot & Stop Card-not-Present Fraud for CNP merchants

A generic training pack developed for managers who train their retail staff to accept CNP transactions. The pack gives best practice guidelines and examines in detail the solutions available to prevent CNP fraud. This pack is available to download as a PDF from www.cardwatch.org.uk.



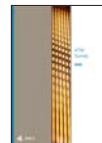
Card Force

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 to share knowledge with other forces.



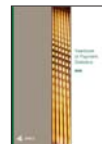
Plastic Card Review

Analyses trends in the use of plastic payment cards in the UK over the past ten years – cost £150.



ATM Survey

Examines the deployment and usage of cash machines in the UK over the past ten years – cost £50.



Yearbook of Payment Statistics

A comprehensive source of UK payment clearing statistics – cost £130.

>> Useful contacts

APACS/Card Watch

020 7711 6259 / 020 7711 6356

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, communications manager

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

DCPCU (media enquiries)

020 7711 6340

Call Credit

0870 060 1414

CIFAS

0870 010 2091

Experian

0870 241 6212

Equifax

0870 514 3700

Royal Mail Customer Enquiries

08457 740740

>> Bank and Building Society Contacts

Abbey

Switchboard: 0870 607 6000

Press office: 020 7756 4223

christina.mills@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
www.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 223 2331
gordon.macmillan@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

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 Holdings

(includes HSBC Bank, HSBC Asset Management, HSBC Investment Banking and Markets and the HSBC Group worldwide)

Switchboard: 0207 991 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

Marks & Spencer Money

Switchboard: 0845 900 0900
Press office: 01244 686669
lucy.cook@mandsmoney.com
liz.neild@mandsmoney.com
www.marksandspencer.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

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
christina.rebollo@rbs.co.uk
www.rbs.co.uk

Standard Chartered

Switchboard: 020 7280 7500
Press office: 020 7280 7163
paul.marriage@uk.standardchartered.com
www.ukstandardchartered.com

Woolwich

Switchboard: 020 8298 5000
Retail press office: 020 7116 6229
ellie.waters@barclays.co.uk
www.woolwich.co.uk

>> Card Scheme Contacts

Visa International

Switchboard: 020 7937 8111

Press office: 020 7937 8111

barderr@visa.com

www.visa.com

MasterCard International

Press office: 0870 990 5403

mastercardpressooffice@webershandwick.com

UK Maestro/Switch/Solo

Press office: 020 7738 6000

johnpinniger@primeword.com

www.switch.co.uk

American Express

Switchboard: 01273 693 555

Press office: 020 7976 4677

paconsultant@aexp.com

www.americanexpress.com

Diners Club

Switchboard: 020 8600 0200

Press enquiries: 020 8600 0200

The Association for Payment Clearing Services (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, card fraud, cheques, electronic payments and cash.

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



© APACS (Administration) Ltd April 2005 (Association for Payment Clearing Services)
Mercury House, Triton Court, 14 Finsbury Square, London, EC2A 1LQ www.apacs.org.uk