CARD FRAUD THE FACTS 2004

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

APACS
Association for Payment Clearing Services

INTRODUCTION

"In 2003 plastic card fraud losses fell for the first time since 1995 and, although this is testament to the efforts of all those involved in card fraud prevention, we cannot afford to become complacent in the fight against the card fraudsters.

The implementation of chip and PIN will play a major part in keeping UK card fraud losses in check – without it losses would be in the region of £1 billion per year by the end of the decade.

Chip and PIN complements our already extensive fraud prevention initiatives, which have succeeded in reducing plastic card fraud growth over the past couple of years. The work of the Dedicated Cheque and Plastic Crime Unit, created in April 2002 to tackle the organised criminal gangs behind the large increases in counterfeit card fraud, has been particularly successful.

Our resolve in confronting this problem remains as strong as ever and we will continue our partnership approach – with the retail industry, law enforcement and the Home Office – to tackle plastic card fraud head-on."

Jon Berrill
Chairman of APACS' Plastic Fraud Prevention Forum

TYPES OF FRAUD

In 2003 plastic card fraud losses decreased for the first time since 1995. The main driver behind this reduction was a fall in cross-border losses on UK cards – down 27 per cent to £94.8 million.

Fraud committed in the UK actually rose by £13 million due mostly to increases in criminals stealing card details to make fraudulent remote transactions – through mail order, telephone, fax and the Internet.

Total: 2003 plastic card fraud on UK-issued cards: £402.4m (-5%)

Contained within this total:

CARD-NOT-PRESENT FRAUD - £116.4m in 2003

Fraud on phone, mail order, fax or Internet transactions

Card-not-present (CNP) fraud is perpetrated through the theft of card details and is now the largest type of card fraud in the UK. Losses in 2003 were £116.4 million, an increase of six per cent on 2002 losses.

The problem in countering this type of fraud lies in the fact that neither the card nor the cardholder needs to be present at the point-of-sale. This means that:

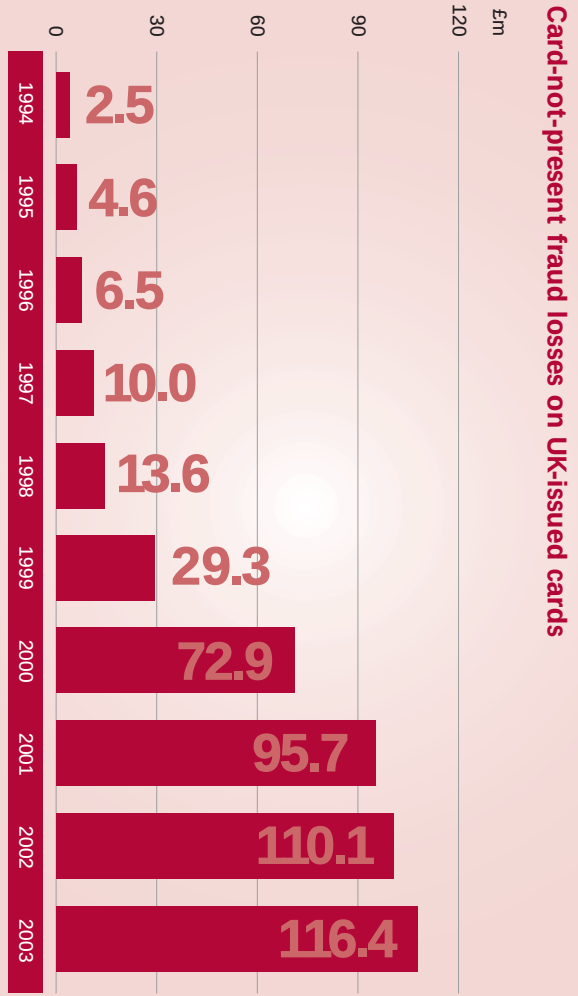
- CNP merchants are unable to check the physical security features of the card to determine if it is genuine
- Without a signature or a PIN it is not easy to confirm the customer is the genuine cardholder
- Card issuers **cannot** guarantee that the information provided in a card-not-present environment relates to the genuine cardholder

A number of initiatives are available to help CNP merchants protect their business from card-not-present fraud (see page 24).

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, fax, mail order or the Internet. As with counterfeit fraud, 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.



COUNTERFEIT CARD FRAUD - £106.7m in 2003

Counterfeit card fraud fell by 28 per cent to £106.7 million in 2003 – the main reason being a £26 million reduction in counterfeit fraud on UK-issued cards used in mainland Europe.

Counterfeit, cloning and skimming of cards still represents a very significant problem, but this is being combatted in the UK by the introduction of chip and PIN (see page 20).

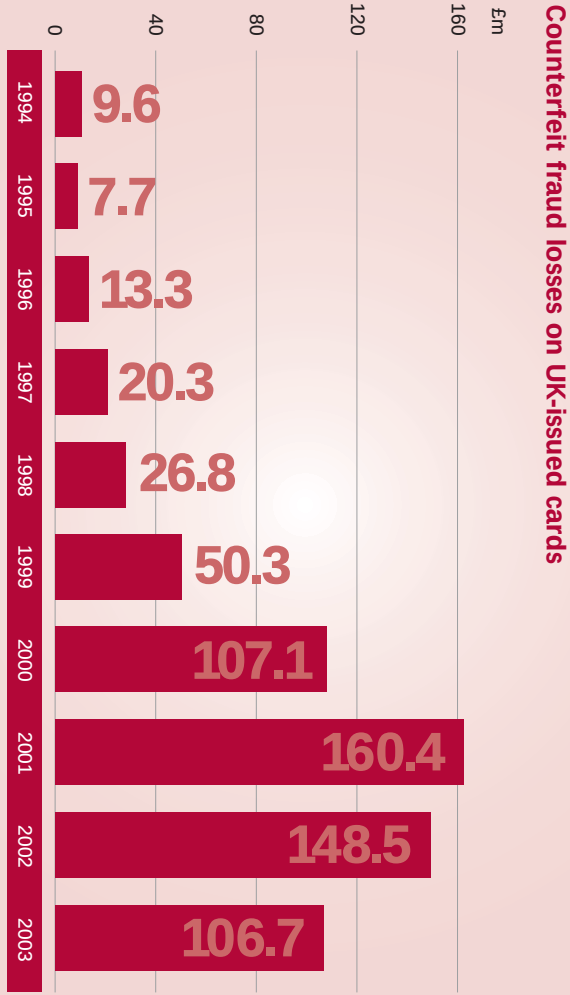
What is counterfeit card fraud?

A counterfeit (cloned) or skimmed card is one that has been printed, embossed or encoded without permission from the issuer, 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 normally 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. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions. Often cardholders are unaware of the fraud until a statement arrives showing purchases they did not make.

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.



LOST AND STOLEN CARD FRAUD - £106.1m in 2003

Fraud on lost and stolen cards amounted to £106.1 million in 2003. This is the second year running that this type of card fraud has reduced.

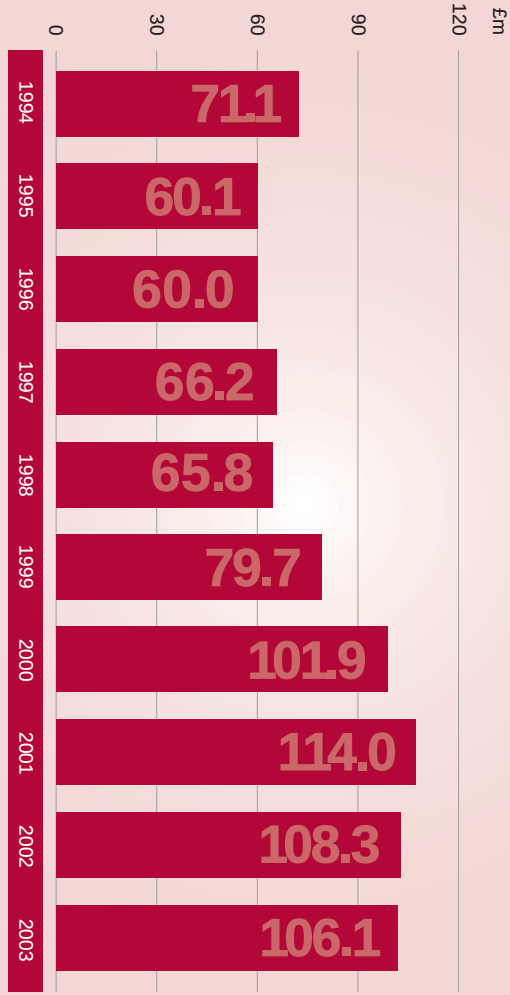
The banking industry has a number of initiatives in place to tackle lost and stolen card fraud:

- 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 (see page 23), run by APACS since 2001, provides help for shop staff on how to detect stolen cards at the point-of-sale.
- Intelligent computer systems that can track customer accounts for unusual spending patterns (see page 26).
- An Industry Hot Card File (see page 28) enables retailers to electronically check whether a card has been reported lost or stolen.

What is lost and stolen card fraud?

This category of fraud occurs 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.



MAIL NON-RECEIPT FRAUD - £43.4m in 2003

This type of fraud increased 17 per cent to £43.4m in 2003, representing just under 11 per cent of total fraud losses.

The banking industry is working with the Royal Mail 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 issuers before cards can be used, or using more secure delivery methods.

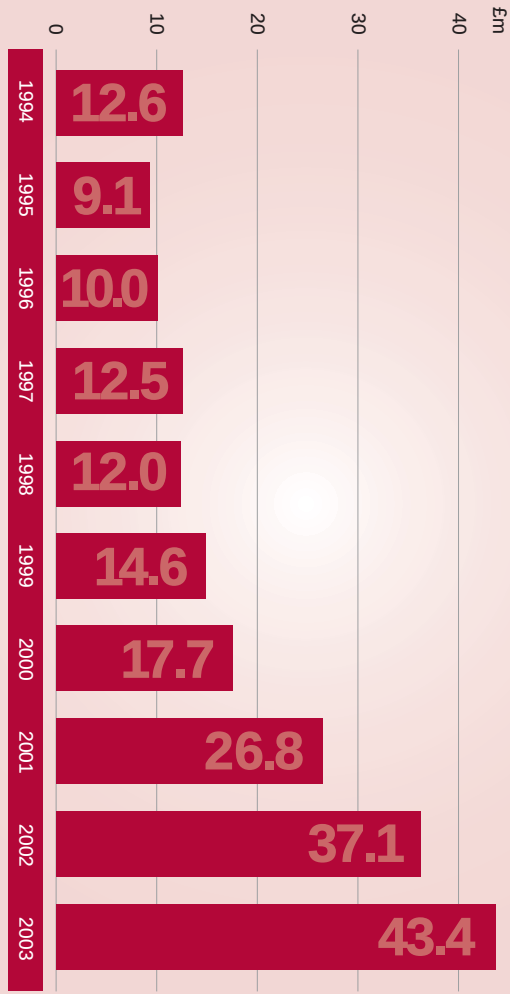
A Mail Non-Receipt Task Force has also been set up by APACS to minimise future fraud growth in this area.

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 receives 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 delivery of a plastic card through the post.

TYPES OF FRAUD



IDENTITY THEFT - £29.7m in 2003

Although identity theft currently accounts for eight 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.

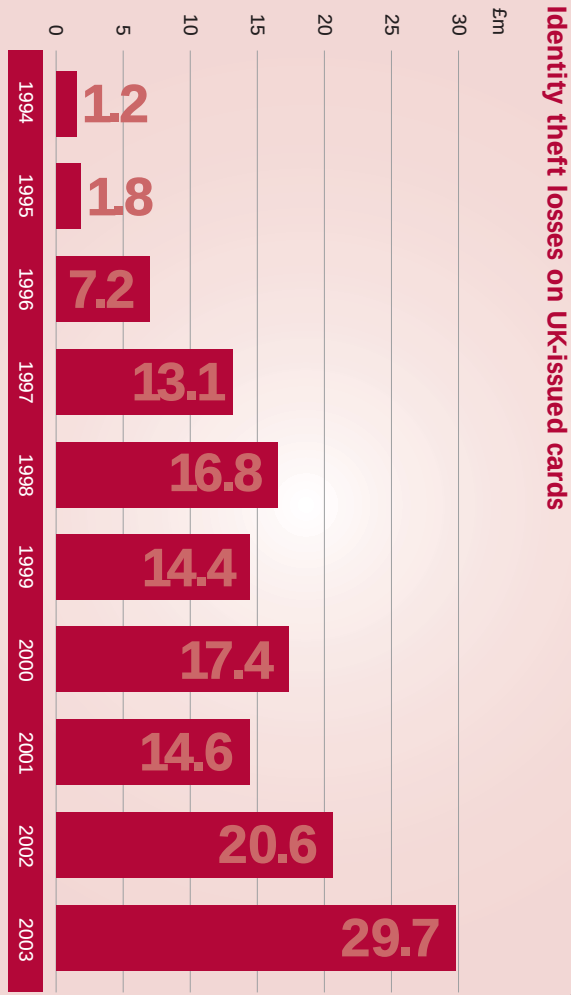
What is identity theft on a card account?

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 (£15.0m in 2003)
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 (£14.7m in 2003)
Criminals take over another person's account, first gathering personal information about the intended victim. The criminal then contacts the card issuer, masquerading as the genuine cardholder, to ask that mail be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent.

Cardholders should discard all personal documentation, especially bank statements, utility bills and receipts, carefully - shred them if possible (see page 36).



WHERE DOES CARD FRAUD TAKE PLACE?

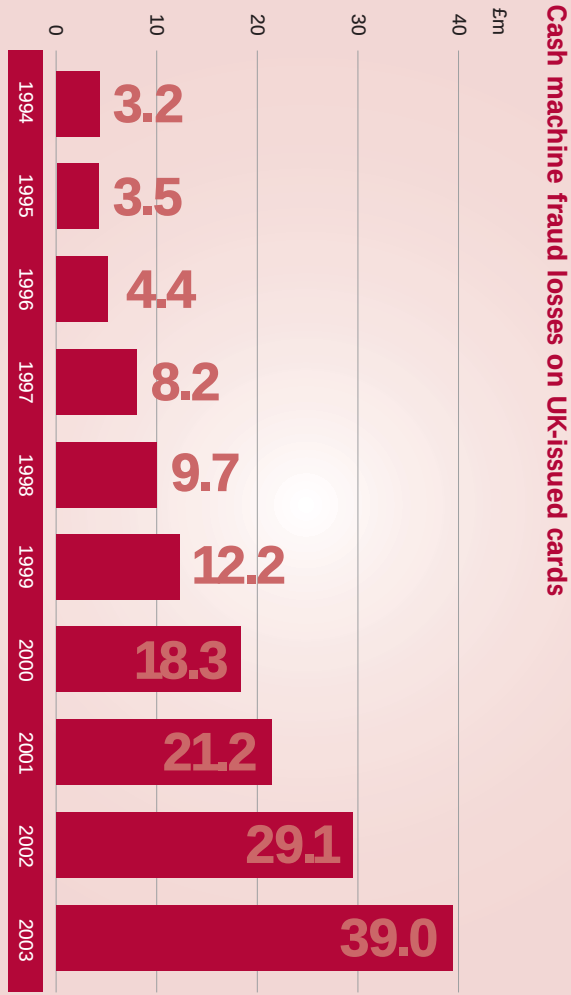
In 2003 most plastic card fraud on UK-issued cards was committed via face-to-face transactions in a shop: £175.1m in 2003 – a fall of six per cent on the previous year. Other locations for fraud include:

CASH MACHINE FRAUD (£39.0m in 2003)

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 five years, it accounts for less than ten per cent of total plastic card fraud losses. PINs kept with cards that are then lost or stolen accounts for a significant portion of these losses.

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

- Shoulder surfing - where 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.
- Skimming at cash machines – a skimming device is attached to the card entry slot 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.



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

- the introduction of chip and PIN, which will effectively prevent the use of skimmed cards in cash machines
- making cash machines tamper-proof
- installing CCTV cameras to deter fraudulent activity
- continued liaison with the police
- siting cash machines in well-lit locations
- placing a safety zone around the machine (a marked area on the pavement for only the cash machine user to stand in)

APACS is also working with cash machine suppliers through its ATM Crime Group to enhance technical solutions available to prevent fraud.

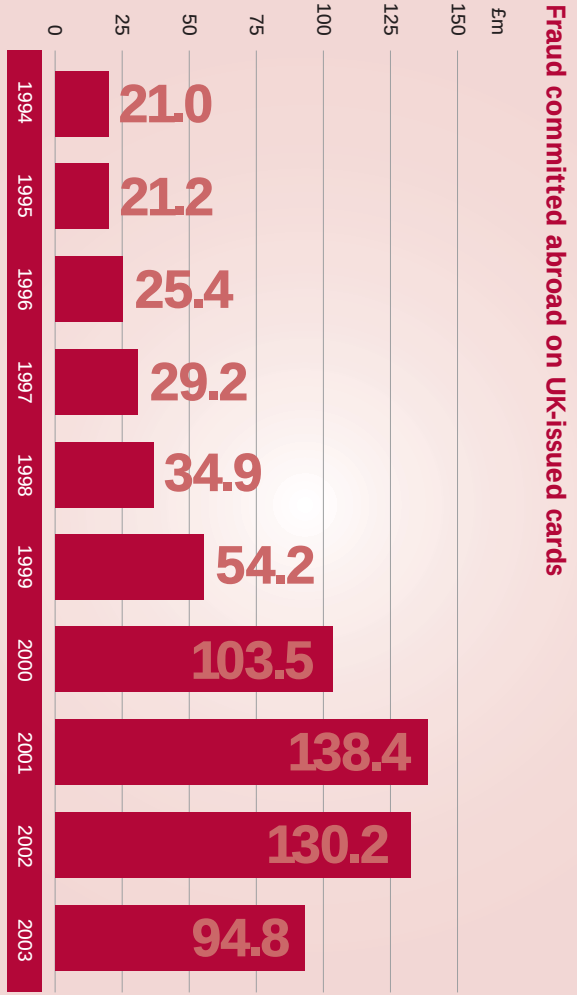
Cardholders should be alert when using cash machines – make sure no-one sees you enter your PIN (see page 34).

FRAUD ABROAD (£94.8m in 2003)

Just under a quarter of fraud on UK cards occurs abroad. Although fraud committed overseas saw dramatic increases between 1998 and 2001, fraud abroad has declined during the past two years, and is the main factor in this year's reduction in total card fraud losses.

Fraud abroad declined by an impressive 27 per cent in 2003. The main reasons for this reduction are:

- the banking industry's increased use of intelligent fraud-detection systems (see page 26)
- the work of the DCPCU (see page 22), which has cracked several counterfeiting groups with international links



Just over half (53 per cent) of fraud abroad took place in three countries – France, Spain and the USA.

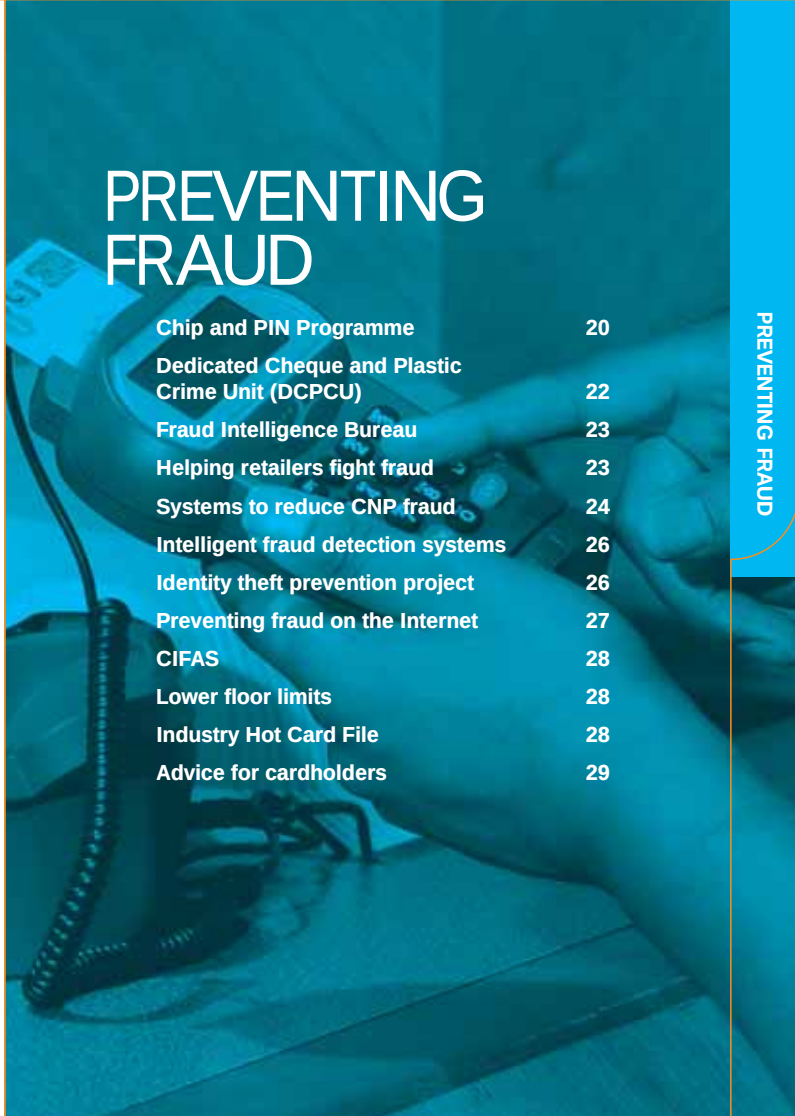
France accounted for 22 per cent (£21.3m) of losses on UK cards used abroad; USA 18 per cent (£16.9m); and Spain 13 per cent (£12.2m). These figures are not just the result of British holidaymakers having their cards stolen in these countries. Most of the fraud on UK cards in these countries is a result of fraudsters using card details taken from people still in the UK, using means such as skimming.

FRAUD ON THE INTERNET/E-COMMERCE FRAUD (£45.0m in 2003)

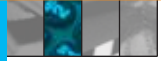
Fraud through e-commerce channels continues to grow, with reliably estimated losses in 2003 of £45m. Most of this type of fraud involves the use of card details fraudulently obtained in the real world to make card-not-present transactions in the virtual world. The incidence of computer hackers stealing and using cardholder data from websites is very low.

A smaller proportion of Internet fraud occurs when the fraudster possesses a genuine card - either through intercepting it in the post or fraudulently applying for it - and chooses to use it to make a card-not-present transaction instead of a card-present transaction in a shop.

The increase in this fraud should be seen in context with Internet usage. Survey data collected for APACS in the latter half of 2003 indicated that there are 30 million adults who use the Internet. Over one-third of adults with access to the Internet have used online banking, and some 18 million purchased goods or services online last year, over 50 per cent more than in 2002.



PREVENTING FRAUD



As the number of cards in issue, and the usage of these cards, continues to grow, it is vital that fraud prevention methods are continually reviewed and developed.

This section details some of these initiatives in more detail:

CHIP AND PIN PROGRAMME

The new, more secure way to pay by plastic

Chip and PIN, a more secure way for more than 42 million UK consumers to use their credit, debit and charge cards, is backed by the UK's banks, building societies, card companies, retailers and card-accepting companies and is co-ordinated by APACS and the British Retail Consortium.

The implementation of chip and PIN in the UK is a revolutionary change for card payments – a change made necessary by ever-increasing levels of plastic card fraud.

It combines two effective security features. The first is a microchip on cards that stores card data more securely than the current magnetic stripe so it is much harder to counterfeit (clone) or skim. The second is the four-digit PIN, which is much harder to copy than a signature and proves you are who you say you are.

Public trial in Northampton

Northampton was selected as the location for a three-month public trial of chip and PIN in 2003. The trial aimed to gauge customer attitudes, help confirm the best ways to rollout the new technology and determine what sort of communications programme would be required to support consumers nationwide.

During this extremely successful trial, 200,000 chip and PIN debit and credit cards were issued to approximately 150,000 customers with around 1,000 retailers taking part.

National roll-out

The success of the trial paved the way for the national roll-out of chip and PIN in the UK, which began in October 2003. The roll-out is taking place throughout the country rather than focusing on any particular area, so cardholders can experience the benefits of chip and PIN regardless of where they live. By December 2004 nine out of ten cardholders should have a chip and PIN card and the majority of transactions in UK shops should be made using chip and PIN.

Chip and PIN for people with a disability

Chip and PIN is good news for customers with disabilities as it enables customers who find signature difficult to use, but find PIN much more convenient, the opportunity to use cards for the first time. Cardholders with a disability who are unable to use a PIN will continue to use signature or whatever method they currently use.

Looking ahead

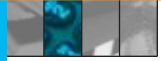
In total there are more than 120 million payment cards to replace, 850,000 shop tills to upgrade and changes to be made in the payment behaviour of 42 million cardholders and 1.5 million retail staff – the investment required to implement the system is estimated to total £1.1 billion.

Most European countries will also be issuing cards to the same global standard as the UK and, over time, there will be increasing use of these cards around the world.

More information about the roll-out of chip and PIN in the UK can be found at **www.chipandpin.co.uk**

Why not photo cards instead of PINs?

Putting identification 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 point-of-sale 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, however, is not sufficiently reliable or cost-effective in a point-of-sale environment to meet the requirements of the UK card industry within the next ten years.

DEDICATED CHEQUE AND PLASTIC CRIME UNIT (DCPCU)

A special police unit combating organised card criminals

The DCPCU was set up in April 2002 as a two-year pilot to focus on the organised criminals behind the huge increases in counterfeit card fraud. The pilot was jointly funded by the Home Office and the banking industry, with APACS and its members also providing fraud investigators and administrative staff to work alongside police personnel.

The Unit has an impressive record of success in identifying, investigating, arresting and prosecuting criminal gangs that perpetrate plastic card fraud. Between April 2002 and January 2004 the Unit recovered more than 35,000 counterfeit cards and compromised card numbers and 2,567 cheques earmarked for fraudulent use. This has led to potential savings of £63.2 million. It has also seized assets and recovered property

PREVENTING FRAUD

valued in excess of £2.1 million from raids on suspected criminals. In the same period 88 people were charged, of whom 35 have been convicted and sentenced to terms of imprisonment.

Going forward, the banking industry has agreed in principle to fund, via APACS, 100 per cent of the costs of a post-pilot DCPCU, which will continue to target the organised gangs responsible for plastic card fraud.

FRAUD INTELLIGENCE BUREAU (FIB)

Exchanging information to fight fraud

The FIB distributes information and intelligence between the banking industry and police to combat counterfeit card fraud, particularly skimming. It has contributed in the identification of several major counterfeiting rings run by organised criminals.

The FIB is also developing its role as a leading centre for the exchange of information and intelligence between police and the banks on all types of card fraud. The FIB works closely with the DCPCU.

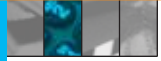
HELPING RETAILERS FIGHT FRAUD

Training and rewarding shop staff for stopping fraud

Tactical programmes to reduce card fraud losses are a core part of the industry's work with fraud-prone card-accepting businesses.

These programmes help create a greater awareness of the problem amongst shop staff and encourage an increase in the number of fraudulent cards captured. Methods used include:

- Incentivising staff through increased and supplemented rewards



- Regular updates to relevant businesses on fraud losses at store level
- The provision of ultraviolet lamps to help identify counterfeit cards.

Underlying these initiatives is APACS' *Spot & Stop Card Fraud* education pack and training programme. Developed in close collaboration with retailers, police and organisations including Crimestoppers, it provides a way to educate retail staff throughout the UK on how to identify counterfeit and stolen plastic cards.

In 2004 an online version of the training pack will become available for participating retailers at **www.cardwatch.org.uk**

Spot & Stop Card Fraud is part of a wider, continuous retailer education programme that incorporates a range of free publications as well as an annual campaign that focuses on current fraud issues affecting retailers and cardholders.

SYSTEMS TO REDUCE CARD-NOT-PRESENT FRAUD

Fighting fraud on phone, mail order and Internet transactions

Although card-not-present fraud – committed over the phone, fax, Internet and by mail order – is increasing, the rate of its growth is declining. (In 1999 and 2000 card-not-present fraud losses increased by 115 per cent and 149 per cent respectively – but in 2003 it grew by only 6 per cent.)

A five-pronged strategy has been implemented 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 them 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's *SecureCode*) for safer online transactions (see page 27).
- A new APACS publication - *Spot & Stop Card-not-Present Fraud* – provides comprehensive fraud prevention training for card-not-present merchants.
- Retailers are encouraged to make use of various card-not-present fraud prevention tools available from third-party providers.
- 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 – a pilot of this initiative will take place during 2004.

Through APACS, a cross-sector working group - involving banks, retailers, card schemes, law enforcement and trade associations - continues to work on system enhancements and new developments to combat card-not-present fraud.

INTELLIGENT FRAUD-DETECTION SYSTEMS

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

The banking industry continues to increase the effectiveness and sophistication of customer-profiling neural network systems that identify unusual spending patterns or high-risk transactions. If irregular spending is detected, card issuers will contact the cardholder to check if the transactions are genuine and, if not, an immediate block can be put on the card. These systems are not only used for transactions taking place in the UK but internationally as well, with considerable success.

IDENTITY THEFT PREVENTION PROJECT

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.

In anticipation of this a multi-sector working group was set up by APACS at the end of 2002 involving the banking industry, British Bankers' Association, CIFAS, key government departments and law enforcement bodies.

In June 2003 APACS published *Identity Fraud – the UK Manual* in conjunction with CIFAS and the Finance & Leasing Association and supported by the Home Office. The *Manual* and its supporting material, including a training programme and best practice guidelines, explain the threat from identity fraud and how businesses and organisations can best protect themselves and their customers.

A Home Office Identity Fraud Steering Committee has subsequently been set up consisting of senior representatives from the public and private sectors, including APACS, who have an interest in reducing identity fraud in the UK.

PREVENTING FRAUD ON THE INTERNET

Secure methods to prevent online transactions

Most Internet fraud involves using card details fraudulently obtained in the real world - such as from carelessly discarded receipts and statements or through corrupt employees in pubs and restaurants copying the details when cards leave the cardholders' sight. 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.

In addition, the international card schemes have made available new security measures to prevent criminals using other people's card details in Internet transactions. *Verified by Visa* and MasterCard's *SecureCode* are personal password-protected services that enable financial institutions to confirm a cardholder's identity for the merchant when that customer is using a card to pay 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, so should reduce fraud abroad as well as domestic fraud.

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

Further details about *Verified by Visa* and *SecureCode* can be obtained from **www.visaeu.com** and **www.mastercard.com/uk**

CIFAS - THE UK'S FRAUD PREVENTION SERVICE

Sharing information to stop fraud

CIFAS provides a range of services to enable its member organisations to exchange information and help identify and prevent fraud, including that relating to plastic cards (see page 38). CIFAS' main emphasis is on identity, application and first-party fraud. 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 distributes data on lost or stolen cards. When a card is swiped as part of a normal transaction, it is automatically checked against the file and an alert is given if the card's details match those on file.

The IHCF contains information on more than 5 million missing cards and over 300,000 cases of attempted fraud were prevented by this system in 2003.

ADVICE FOR CARDHOLDERS

In general:

- Guard cards and card details. Don't let them out of your sight when making a transaction.
- Don't carelessly discard receipts from card transactions. If possible, 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.
- When using a cash machine, be wary of anyone trying to watch you enter your PIN and do not allow yourself to be distracted.
- Report lost or stolen cards or suspected fraudulent use of your card account to your card issuer immediately. The 24-hour emergency number is on your last statement or call directory enquiries.

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

- Don't give your card number 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 may be asked for information including the card number, expiry date, the three or four-digit card security code on the signature strip, issue number where applicable, and your name as it appears on your card.

- 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 that is being 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 issuer carefully as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. Contact your card issuer 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 issuer immediately. You may be asked to sign a disclaimer, confirming that you did not undertake the transaction.

Computer protection when using the Internet:

- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- 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.
- Two of the most popular browsers are Microsoft Internet Explorer and Netscape Navigator. Check that you are using a recent version - you can usually download the latest version from these browsers' websites.

Safe Internet shopping with your cards:

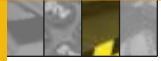
- Only shop at secure websites - ensure that the security icon, the locked padlock or unbroken key symbol, is showing in the bottom right of your browser window before sending your card details. The beginning of the retailer's Internet address will change from 'http' to 'https' when a purchase is made 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 – always be wary of e-mails asking you to click on a link or confirm your details. 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). 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.
- Check statements from your card issuer 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 issuer immediately.
- If you have any doubts about giving your card details, find another method of payment.
- If you regularly make transactions over the Internet consider opening a separate credit card account specifically for these transactions.

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

Advice when choosing your PIN:

- Do not use a number or numbers that can obviously be associated with you - for instance your telephone number, birthday, your street number, driving licence number or popular number sequences (such as 9876 or 1234 or 9999).
- 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 a combination of double numbers e.g. 77 along with two others that have some meaning for you. Remember never to write your PIN down and never disclose it to anyone even if they claim to be from your bank or the police.



Keeping your PIN a secret:

- Do not allow anyone else to use your card, PIN or other security information.
- Always memorise your PIN and other security information and destroy the notification as soon as you receive it. If the PIN you are provided with 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:

Using a cash machine is a very safe way of withdrawing cash and accessing banking services although, unfortunately, criminals do target cash machines. The following advice for cardholders using cash machines 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 close to the cash machine is behaving suspiciously or makes you feel uncomfortable choose another.
- If there is 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 aware of your surroundings. 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 and always shield the keypad to avoid anyone seeing you enter your PIN.

Leaving a cash machine

- Once you have completed a transaction, discreetly 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.
- Make a note of your card issuers' 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 you should inform your bank or card issuer immediately.
- If someone else uses your card before you tell your card issuer 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 shown 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 part of the losses. You would probably still have your card in your possession if you are a victim of card-not-present fraud or if your card has been counterfeited.

ID fraud – tips to help keep your identity safe:

- Always keep personal documents, plastic cards and cheque books in a safe and secure place. Keep cheque books 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. 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 e-mails requesting information. If in doubt, 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 issuer 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. If you fail to receive a bank statement, card statement, utility bill or other financial information contact the supplier. How easy would it be for somebody to intercept your post? 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).

CARDHOLDER ADVICE

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: 08705 143700 (**www.equifax.co.uk**)
  Call Credit: 0870 060 1414 (**www.callcredit.co.uk**)
- 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.

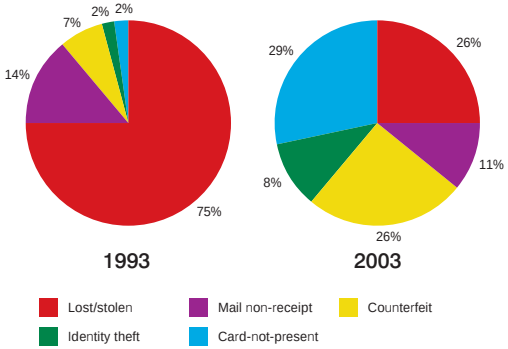
CARD FACTS AND FIGURES

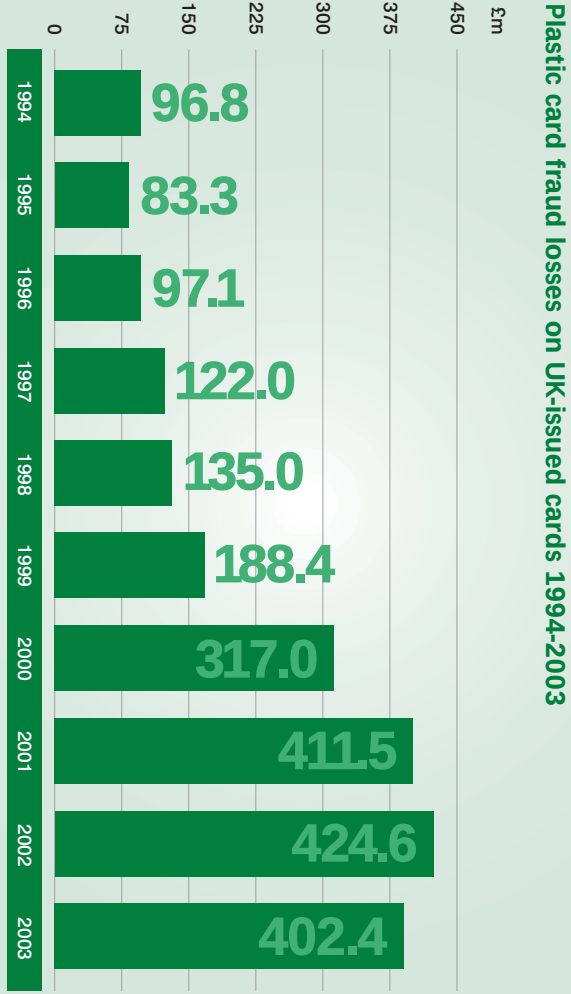
(AS OF 31 DEC 2003)

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 0.13 per cent – are significantly less than the 1991 peak level of 0.33 per cent. This fraud-to-turnover ratio fell from 0.164 per cent in 2002 – a reduction all the more remarkable when the 5 per cent fall in fraud is viewed in the light of a 9 per cent increase in the number of card transactions and a 12 per cent increase in the value of card transactions during 2003.

The following pie charts illustrate how the trends of card fraud losses have changed over the last ten years. Counterfeit card fraud and fraud committed through phone, mail order, fax and Internet – when the card is not present – have increased significantly. The proportion of fraud committed on lost and stolen cards is steadily decreasing.





Annual plastic card fraud losses on UK-issued cards 1994-2003

All figures £m	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Type of fraud										
Lost/Stolen	71.1	60.1	60.0	66.2	65.8	79.7	101.9	114.0	108.3	106.1
Mail non-receipt	12.6	9.1	10.0	12.5	12.0	14.6	17.7	26.8	37.1	43.4
Counterfeit	9.6	7.7	13.3	20.3	26.8	50.3	107.1	160.4	148.5	106.7
Card-not-present	2.5	4.6	6.5	10.0	13.6	29.3	72.9	95.7	110.1	116.4
Identity theft	1.2	1.8	7.2	13.1	16.8	14.4	17.4	14.6	20.6	29.7
Fraud in the UK	76.0	62.1	71.6	92.8	100.1	134.1	213.4	273.0	294.4	307.6
Fraud abroad	21.0	21.2	25.4	29.2	34.9	54.2	103.5	138.4	130.2	94.8
Total	96.8	83.3	97.1	122.0	135.0	188.4	317.0	411.5	424.6	402.4

Plastic card fraud losses on UK-issued/UK-acquired cards in 2003

Regional hot spots

Region	£m
South East	161.0
North West	20.8
West Midlands	19.2
Yorkshire & Humberside	14.9
East Midlands	14.3
Scotland	12.4
South West	9.5
East Anglia	5.7
North East	5.5
Wales	5.5
Northern Ireland	1.1

PLASTIC CARD FACTS AS OF 31 DECEMBER 2003

- Credit cards were first issued in the UK in 1966 and debit cards in 1987
- There are more than 160 million plastic cards (147 million in 2002) in issue in the UK:
  62.9 million debit cards (59.4 million in 2002)
  66.8 million credit cards (58.8 million in 2002)
  24.9 million stand-alone cash machine cards (23.2 million in 2002)
  4.4 million charge cards (4.3 million in 2002)
  1.6 million cheque guarantee cards (1.8 million in 2002)
- Over 7.7 billion transactions were made on UK cards in 2003
- The total value of all transactions reached £420 billion in 2003
- Debit cards were used 3.4 billion times for purchases with a value totalling over £130 billion in 2003
- Credit and charge cards were used 1.8 billion times for purchases with a value of £113 billion in 2003
- There were 107 debit card payments per second in 2003 compared with 58 credit/charge card payments per second
- The average purchase value on a UK-issued credit card in the UK is around £57
- The average purchase value on a UK-issued debit card in the UK is £39
- 39% of all debit card payments are made in supermarkets
- The number of transactions abroad on UK-issued cards increased by eight per cent in 2003 to 230 million

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 used to withdraw cash
- There are 46,461 cash machines in the UK – up from 40,825 in 2002
- In 2003 there were 2.37 billion cash withdrawals from cash machines in the UK – an average of 75 per second
- The total value withdrawn from cash machines in the UK in 2003 was £144.1 billion – an average of £4,750 per second
- The average cash withdrawal at a cash machine is £61
- 31.6 million adults in the UK are regular cash machine users

PLASTIC CARD FRAUD FACTS

- £402.4 million was lost to card fraud in 2003
- More than £1.1 million worth of card fraud occurs on UK plastic cards every day. A fraudulent transaction takes place every eight seconds
- Nearly 57 per cent of all fraudulent card use in the UK takes place at the retail point-of-sale
- In 2003 the average loss per fraudulent case was £653
- In 2003 the average value of a fraudulent transaction was £111
- If chip and PIN was not put into action, forecasts estimate that UK card fraud losses would be in the region of £1 billion by the end of the decade

GLOSSARY

authorisation

The process whereby a merchant (or a cardholder through a cash machine) requests permission for the card to be used for a particular transaction.

biometrics

Biometric methods of identification work by measuring unique human characteristics as a way to confirm identity. Examples are finger or iris scanning or dynamic signature verification.

card issuer

A bank, building society or other financial institution that issues payment cards, cash machine cards or cheque guarantee cards to its customers. For payment cards, the card issuer undertakes responsibility to settle transactions made with the card (except in some cases where fraud is present).

card-not-present (CNP)

A transaction where the merchant, retailer or other service provider does not have physical access to the payment card; examples are transactions by phone, fax, mail order or Internet.

card schemes

Card schemes set the business rules that govern the issue of the payment cards that carry their logo. Typically, these rules apply throughout the world to ensure interoperability of cards. In many countries, domestic schemes also operate. The schemes operate the clearing and settlement of payment card transactions. In the UK, banks and building societies must be members of the appropriate scheme to issue cards and acquire card transactions. Examples of international card schemes in the UK are Visa, MasterCard, American Express and Diners Club. Switch is a UK domestic debit card scheme.

Card Security Code (CSC)

The last three or four digits of a number printed on or just below the signature panel on payment cards – this code was formerly called the CV2.

charge card

A payment card, enabling holders to make purchases and to draw cash up to a pre-arranged ceiling, the terms of which include the obligation to settle the account in full at the end of a specified period. Cardholders are normally charged an annual fee.

cheque guarantee card

Also known as a cheque card. A card issued by a bank or building society for the purpose of guaranteeing payment by, or supporting the encashment of, a cheque up to a specified value (£50, £100 or £250). All cheque guarantee cards in the UK Domestic Cheque Guarantee Card Scheme depict the bust of William Shakespeare in either the cheque guarantee hologram or logo on the card.

chip card

Also known as an integrated circuit (IC) or smart card. A chip card holds details on a secure computer microchip that can store and process information. Chip cards usually also have a magnetic stripe.

FACTS AND FIGURES

counterfeit (cloned/skimmed) card

A dummy or fake card that has been printed, embossed or encoded so as to appear to be a legitimate card, or a card that has been validly issued but subsequently altered or re-encoded.

credit card

A payment card enabling holders to make purchases and to draw cash up to a pre-arranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, in which case interest is charged. In the case of cash withdrawals, interest is normally charged from the transaction date. Cardholders may be charged an annual fee.

debit card

A payment card linked to a bank or building society account, used to pay for goods and services by debiting the holder's account; usually also combined with other facilities such as cash machine and cheque guarantee functions.

electronic commerce (e-commerce)

Transactions that are conducted over an electronic network where the buyer and merchant are not at the same physical location e.g. plastic card transactions via the Internet.

electronic purse

Also known as e-purse or a pre-payment card. A stored-value payment card used to pay for goods and services. It is an alternative to cash. The card can be disposable or reloadable. The stored value is reduced as payments are made.

EMV

The internationally agreed standards for chip payment cards, originally agreed by Europay, MasterCard and Visa. EMV standards are maintained by EMVCo, an organisation owned and managed by MasterCard and Visa.

encryption

A method of making information secret, so that only a person who knows the necessary key or password can understand or decrypt the information.

floor limit

A limit on the value of each transaction, agreed between the merchant and acquiring bank, above which authorisation must be obtained by the merchant.

Industry Hot Card File (IHCF)

A computerised list of reported lost and stolen cards, available to merchants to assist in the identification and prevention of fraudulent transactions.

intelligent detection systems

Computer systems developed by the banking industry to help identify fraudulent card use. Also known as knowledge-based systems and neural networks.

magnetic stripe

The magnetic stripe that currently appears on the back of all payment cards issued by financial institutions. It contains essential customer and account information, most of which is usually also embossed on the card.

MasterCard

An international card scheme.

PIN (personal identification number)

A set of numeric characters, usually a four-digit sequence, used by the cardholder to verify identity at the point-of-sale or a customer activated device, such as a cash machine. The number is generated by the card issuer using a secure computerised process when the card is first issued and may be changed by the cardholder thereafter.

PIN pad

The numeric pad into which a cardholder enters their PIN to authorise a transaction. PIN pads may be fixed or portable.

PMO

Programme Management Organisation. An independent, not-for-profit body responsible for co-ordinating the chip and PIN project on behalf of the banking and retailer industries.

point-of-sale (POS)

The physical location, such as a check-out, till or sales point, where a customer pays for goods or services.

skimming

The most prevalent form of counterfeit fraud whereby a card's magnetic stripe details are electronically copied without the legitimate cardholder's knowledge and put onto another card.

Visa

An international card scheme.

USEFUL CONTACTS

APACS / Card Watch

Switchboard
020 7711 6200

Sandra Quinn, director of corporate communications
020 7711 6234
07768 044656
sandra.quinn@apacs.org.uk

Jemma Smith, communications manager
020 7711 6340
07811 113075
jemma.smith@apacs.org.uk

Catherine Wike, PR executive
020 7711 6368
catherine.wike@apacs.org.uk

Mark Bowerman, communications executive
020 7711 6251
mark.bowerman@apacs.org.uk

www.apacs.org.uk
www.cardwatch.org.uk

BANK AND BUILDING SOCIETY CONTACTS

ABBEY

Switchboard: 0870 607 6000
Press office: 020 7756 4223
Press office fax: 020 7756 5632
christina.mills@abbey.com
www.abbey.com

ALLIANCE & LEICESTER

Switchboard: 0116 201 1000
Press office: 0116 200 3355
Press office fax: 0116 200 2701
pressoffice@alliance-leicester.co.uk
www.alliance-leicester-group.co.uk

BANK OF ENGLAND

Switchboard: 020 7601 4444
Press office: 020 7601 4411
Press office fax: 020 7601 5460
press@bankofengland.co.uk
www.bankofengland.co.uk

BANK OF SCOTLAND (HBOS)

Switchboard: 0870 600 5000
Press office: 0131 243 7077
Press office fax: 0131 243 7082
pressoffice@hbosplc.com

BARCLAYS BANK inc BARCLAYCARD

Switchboard: 01604 234 234
Press office: 01604 251 229
Press office fax: 01604 253 499
mark.gonnella@barclaycard.co.uk
www.barclaycard.co.uk

CAPITAL ONE

Switchboard: 0115 843 3300
Press office: 0115 843 3174
Press office fax: 0115 843 3186
richard.holmes@capitalone.com
www.capitalone.co.uk

CITIGROUP

Switchboard: 020 7500 5000
Press office: 020 7986 5602
Press office fax: 020 7986 5610
jeremy.hughes@citigroup.com
www.citigroup.com

CLYDESDALE BANK

Switchboard: 0141 248 7070
Press office: 0141 223 2555
Press office fax: 0141 223 2559
gordon.macmillan@eu.nabgroup.com
www.cbonline.co.uk

CO-OPERATIVE BANK

Switchboard: 0161 832 3456
Press office: 0161 829 5397
Press office fax: 0161 839 4220
dave.smith@co-operativebank.co.uk
www.co-operativebank.co.uk

COUTTS GROUP

Switchboard: 020 7753 1000
Press office: 020 7957 2427
Press office fax: 020 7753 1042
julie.cooper@coutts.com
www.coutts.com

EGG

Switchboard: 020 7526 2500
Press office: 020 7526 2600
Press office fax: 020 7526 2604
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
Press office fax: 01422 333 007
markhemingway@halifax.co.uk
www.hbosplc.com

HFC BANK

Switchboard: 01344 890 000
Press office: 01344 892 571
Press office fax: 01344 892 646
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: 020 7260 9000
Press office: 020 7991 0641
Press office fax: 020 7991 4883
pressoffice@hsbc.com
www.hsbc.com

LLOYDS TSB BANK

Switchboard: 020 7626 1500
Press office: 020 7356 2493
Press office fax: 020 7356 2494
mary.walsh@lloydstsb.co.uk
www.lloydstsb.com

MARKS & SPENCER MONEY

Switchboard: 0845 900 0900
Press office: 01244 686669
louis.hill@marks-and-spencer.com
www.marksandspencer.com

MBNA EUROPE BANK

Switchboard: 01244 672 000
Press office: 01244 574404
Press office fax: 01244 574 153
john.greaves@mbna.com
www.mbna.com

MORGAN STANLEY

Switchboard: 020 7425 8000
Press office: 020 7425 8005
tim.roe@morganstanley.com
www.morganstanley.com

NATIONAL AUSTRALIA BANK

Switchboard: 020 7710 2100
Press office: 020 7710 2435
Press office fax: 020 7796 3202
ken.pipe@eu.nabgroup.com
www.national.com.au

NATIONWIDE

Switchboard: 01793 513513
Press office: 01793 655 198
Press office fax: 01793 655 045
pressoffice@nationwide.co.uk
www.nationwide.co.uk

NATWEST GROUP

Switchboard: 020 7920 5555
Retail bank press office: 020 7672 1931
Press office fax: 020 7672 1934
ronan.kelleher@natwest.com
www.natwest.com

NORTHERN ROCK

Switchboard: 0191 285 7191
Press office: 0191 279 4676
Press office fax: 0191 279 4200
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
Press office fax: 020 7672 1934
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 7699 4077
Retail press office fax: 020 7699 3644
perry.jones@barclays.co.uk
www.woolwich.co.uk

CARD SCHEMES CONTACTS

VISA INTERNATIONAL

Switchboard: 020 7937 8111
Press office: 020 7937 8111
Press office fax: 020 7795 5739
barderr@visa.com
www.visa.com

MASTERCARD INTERNATIONAL

Press office: 020 7282 2921
james.mcdonald@citigatedr.co.uk
www.mastercard.com

SWITCH

Switchboard: 020 7330 0700
Press office: 020 7330 0700
Press office fax: 020 7330 0707
scsl@switch.co.uk
www.switch.co.uk

AMERICAN EXPRESS

Switchboard: 01273 693 555
Press office: 020 7976 4677
Press office fax: 020 7976 4419
jacqueline.a.goozee@aexp.com
www.americanexpress.com

DINERS CLUB

Switchboard: 020 8600 0200
Press enquiries: 020 8600 0220
Press office fax: 020 8600 0373
phil.percival@dinerseurope.com

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
visit www.cardwatch.org.uk
e-mail cardwatch@apacs.org.uk
call 020 7711 6251

APACS
Association for Payment Clearing Services

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