The Association for Payment Clearing Services (APACS) is a non-statutory association of major banks and building societies and has become the umbrella body at the heart of the UK payments industry. APACS provides the forum for banks and building societies to discuss non-competitive issues relating to money transmission, including the prevention of plastic card fraud.

APACS' Plastic Fraud Prevention Forum (PFPF) represents all of the UK's major card issuers and works to develop card fraud prevention initiatives.

Card Watch is the PFPF's public awareness campaign and the focus for co-ordinated activities to combat card fraud.

For further information about Card Watch visit **www.cardwatch.org.uk**, email **cardwatch@apacs.org.uk** or call **020 7711 6356**.

(Association for Payment Clearing Services)
Mercury House, Triton Court, 14 Finsbury Square, London EC2A 1LQ

t 020 7711 6251
f 020 7628 0927
www.apacs.org.uk

APACS

Card Fraud

the facts 2002

Contents

APACS' card fraud public awareness campaign is called Card Watch.
For further information visit **www.cardwatch.org.uk,** phone **020 7711 6356**
or email **cardwatch@apacs.org.uk.**

Overview

The Association for Payment Clearing Services (APACS) has prepared this booklet to provide an overview of plastic card fraud and its prevention in the UK.

Card fraud cost the UK £411.4 million in 2001 – an increase of 30 per cent on the 2000 figure of £317.0 million*. Most types of fraud are continuing to grow, such as counterfeit and the fraudulent use of card details in transactions made by telephone, mail order or internet.

To combat plastic card crime, two facts need to be established at the time of a transaction – that the card is the genuine item and that the person using it is the true owner.

The introduction of highly-secure chip cards in the UK meets the first of these objectives by confirming that a card is not a counterfeit. Chip cards also open up new possibilities for tackling the second objective for fraud prevention – identifying the cardholder.

To fulfil this second part, the banking industry has committed to ensuring that by 2005 all face-to-face UK credit and debit card transactions will be authorised by the customer keying in their PIN (personal identification number) rather than by signing a receipt.

This is a revolutionary change for the card payment system in this country. Over the next two to three years more than 100 million UK debit, credit and charge cards will be reissued containing microchips that are capable of identifying cardholders using a PIN.

Against a backdrop of shared concern between the banks, retailers, police and the Home Office, card fraud prevention efforts also continue on a range of short-term initiatives before the longer term benefits associated with chip and PIN cards can be realised.

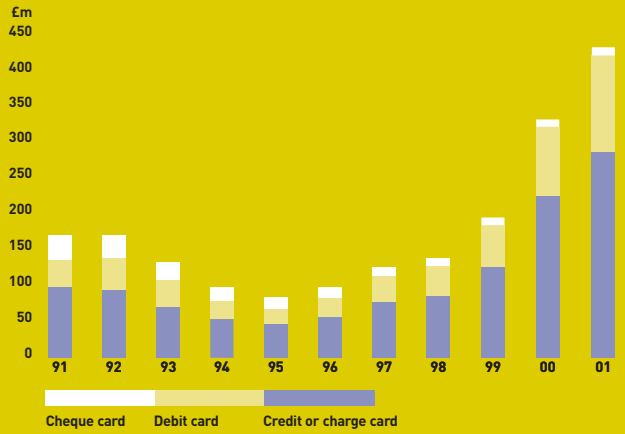
*Prior to 2000, fraud figures were calculated as net/gross. From 2000 onwards, the figures are gross only. Original 2000 figure of £292.6 million (published by APACS last year) has been adjusted from net/gross to a gross figure of £317.0 million, in order to provide a direct comparison with the 2001 figure.

The facts about card fraud

Plastic card fraud losses have risen significantly in the UK in recent years, as they have in most countries around the world. To put this fraud into context, it should be noted that card usage and the number of cards issued continues to rise in the UK. As a result, plastic card fraud losses against total turnover – at 0.183 per cent – are only just over half the 1991 peak level of 0.33 per cent.

The following graph shows the pattern in total fraud losses over the last eleven years broken down by card type.

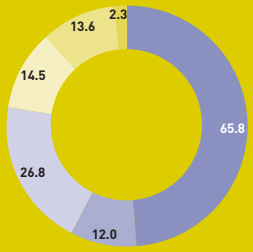
Plastic card fraud losses 1991-2001



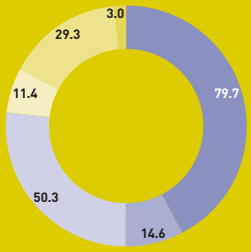
The pattern of fraud shows a steep reduction in losses from the early to mid-1990s, as a result of a range of bank and retailer partnership prevention initiatives, and then a resurgence to 2001. This is due to criminals adapting their methods, resulting in a large growth in fraudulent usage of card details and counterfeit fraud.

The following pie charts illustrate how the trends for card fraud have changed since 1998, detailing the amounts lost to specific types of fraud.

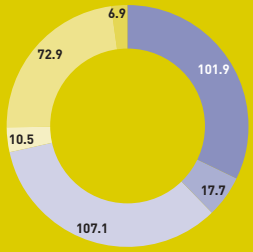
The pie charts below show that the proportion of fraud on lost or stolen cards is decreasing. Counterfeit fraud and fraudulent use of card details through phone, mail order and internet are increasing steeply.



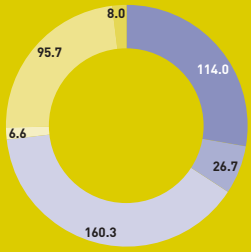
1998: £135 million



1999: £188.4 million



2000: £317 million



2001: £411.4 million

Fraud abroad

One-third of fraud on UK cards occurs abroad. More than half of this fraud takes place in three countries: the United States (19 per cent of losses on UK cards used abroad), France (17 per cent) and Spain (16 per cent). Fraud committed abroad on UK cards in 2001 increased by 34 per cent on the previous year's figure, costing £138.4 million.

Some major factors behind the increase are that UK fraud prevention initiatives have driven criminals abroad and advances in technology have made it easier for organised criminal gangs to move information around the world. APACS and its member banks and building societies are continuing to work closely with Visa and Europay/MasterCard on cross-border fraud initiatives.

Types of fraud

The types of fraud used by card criminals:

1 Counterfeit fraud
Counterfeit card fraud cost £160.3 million in 2001, an increase of 50 per cent on losses of £107.1 million in 2000. A counterfeit card is either one that has been printed, embossed or encoded without permission from the issuer, or one that has been validly issued and then altered or re-coded.

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 the cardholder is unaware of the fraud until a statement arrives showing purchases they did not make.

Cardholders should always keep their card in sight when making a transaction

2 Fraudulent use of card details

Fraud on phone, mail order or internet transactions

Card-not-present fraud cost £95.7 million in 2001 and occurs when neither the card nor its holder is present at the point-of-sale, as happens in telephone, fax, mail order and internet transactions.

This crime involves using fraudulently obtained card details to make a purchase. Usually the details are taken from discarded receipts or copied down without the cardholder's knowledge. As with counterfeit fraud, the legitimate cardholder may not be aware of the fraud until a statement is received.

The UK card industry has made available to merchants an address and card security code checking system to fight this type of fraud (see page 13).

Discard receipts carefully – shredding them if possible – and check statements for any unfamiliar transactions

3 Lost or stolen cards

Fraud on lost or stolen cards cost £114 million in 2001, an increase of 12 per cent on the previous year. Most fraud on lost or stolen cards takes place at retail outlets before the cardholder has reported the loss. In other cases, the card details from lost and stolen cards are used to make fraudulent card-not-present transactions.

A hot card file system is used to distribute data about lost or stolen cards to 80,000 retailers in the UK to alert them to cards reported missing.

To help detect fraud on cards that are not yet reported missing, the banking industry uses intelligent computer systems that track customer accounts for unusual spending patterns (see page 14).

It is vital that cardholders keep cards safe at all times, and report missing cards to their issuing bank immediately so a block can be put on the card

4 Mail non-receipt fraud
The number of plastic cards stolen in the post peaked in 1991 when this type of fraud cost the industry £33 million and represented 20 per cent of total fraud losses. At this point the banking industry formed an ongoing partnership with the Post Office to control card distribution, reducing this type of fraud considerably.

Although still a small category of fraud, there was a significant increase in 2001 to £26.7 million – six per cent of total fraud losses. This increase illustrates how criminals constantly look for other areas to exploit as fraud prevention initiatives drive them away from their usual methods.

Contact your issuing bank if you are concerned about the delivery of a plastic card through the post

5 Identity theft
Although evidence of identity theft on card accounts is currently minimal, the UK banking industry is preparing for a possible rise once the chip and PIN system makes its impact since this could drive criminals to look for different ways to perpetrate fraud.

There are two categories of identity theft that together cost an estimated £12 million in 2001. They comprise £6.6 million for application fraud and an estimated £5 million for account take-over.

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

Types of fraud (cont)

Account take-over
Criminals try to take over another person's account, first by gathering 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 bank statements, utility bills and receipts carefully – shredding them if possible

6 ATM (automated teller machine) fraud
ATM fraud is not a type of fraud but the location where it occurs, usually with lost and stolen cards. Most cases of ATM fraud occur when the legitimate cardholder has written down their PIN and kept it with their card in a purse or wallet that is stolen.

An increasingly common problem is shoulder surfing – where criminals look over a cash machine user's shoulder to watch them enter their PIN, then steal the card using distraction techniques or pickpocketing.

ATM fraud that involves card-trapping devices is also on the rise. The device retains the card inside the ATM, at which point the criminal approaches the victim and tricks them into re-entering the PIN. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.

ATM fraud cost the industry £21.2 million in 2001, five per cent of total fraud losses.

Never write down your PIN and be alert when using cash machines

Preventing fraud

With society's reliance on cards becoming more widespread and levels of organised card crime rising, losses from card fraud are on the increase too. It is vital that fraud prevention methods are continually developed and reviewed to maintain low levels of fraud growth as a percentage of plastic card turnover.

Chip and PIN system by 2005

Secure payment cards that fight fraud

The UK banking industry began its roll-out of 'smart' chip cards in spring 1999. The industry is complementing this with the introduction of a fraud-fighting programme to ensure that, by 2005, all UK credit and debit card transactions will be authorised by the customer keying in their PIN rather than by signing a receipt.

This signals the beginning of a revolutionary change for the UK card payment system. Using a better method of identifying the cardholder combined with the chip's ability to verify that the card is authentic will drastically improve security and significantly reduce most types of card fraud.

Investing in the future

The investment required to implement a chip and PIN system will cost UK banks and retailers approximately £1.1 billion.

Working together, banks and retailers will need to upgrade or replace more than 100 million debit and credit cards, 750,000 point-of-sale terminals and 37,000 cash machines.

In addition to upgrading systems, banks and retailers will need to educate and help 42 million shared customers to use PIN rather than signature, and guide them through the transition process.

How chip cards work

A chip card can be recognised by the gold or silver coloured contact plate on the front of the card, which contains a microchip with highly secure memory and processing capabilities. Cardholders use them in the same way as existing credit, debit and ATM cards.

Chip cards will still have a magnetic stripe on the back for a number of years to ensure that cards can continue to be used abroad.

The personal data contained in the chip is the same as that held on the existing magnetic stripe and covers such details as cardholder name, card number and expiry date. The information is stored more securely in the chip to safeguard against counterfeiting.

International use

To ensure chip cards are recognised and accepted in all countries where card payments are made, countries around the world are building them to an international specification set by the international card schemes Europay, MasterCard and Visa (EMV).

The UK is at the forefront of an international roll-out of EMV-compliant chip technology. Already there are more than 25 million chip cards in issue in the UK and, by the end of the year, it is estimated that more than half of the UK's 108 million credit, debit and charge cards will contain chips.

Benefits of chip cards

Initially, the major advantage of chip cards is increased security against counterfeit fraud: a rapidly growing crime in the UK and around the world. Chip technology uses highly sophisticated processing to identify genuine cards and make counterfeiting much more difficult, and hugely expensive, for criminals.

Chip cards have the potential to be used with chip readers attached to personal computers, mobile phones or digital televisions, making on-line transactions of the future even more secure.

The increase in security that chip and PIN cards bring may also lead to retailers expanding their use of unattended payment terminals in petrol stations, car parks and self-scanning at supermarkets.

The sophistication of chip technology also provides an excellent foundation for using PINs as the method of identifying cardholders at point-of-sale.

Why not photo cards instead of PINs?

Putting identification photographs on cards has been considered as an additional security method, but this would only provide costly short to medium-term relief. With the introduction of PINs, the banking industry is shifting the responsibility of identifying the cardholder away from point-of-sale staff by relying on technology-based methods to help prevent fraud.

What about identification methods like iris scanning?

The memory capacity of the chip 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 promoted as possibilities. However, such technology is not sufficiently reliable or cost-effective to meet the requirements of the UK card industry within the next ten years.

PINs will be used to identify cardholders in the medium term.

Specialist police unit to fight card crime

Pilot of a dedicated cheque and plastic crime unit

There is strong evidence that organised criminals use counterfeit card fraud as a high-profit enterprise to help fund other serious crime. This led APACS, the Association of Chief Police Officers and the Home Office to launch a two-year pilot of a dedicated cheque and plastic crime unit in April 2002 to focus on such crime syndicates.

The unit aims to fight organised crime that involves plastic and cheque fraud and, by association, other connected crimes such as drug trading. If the unit is considered a success when the pilot ends, it has the potential to become permanent.

The dedicated unit is based in London but will work across different police force borders in England and Wales as necessary in investigations.

Fraud Intelligence Bureau (FIB)

Exchanging information to fight fraud

Based at APACS, the FIB shares information and intelligence between the banking industry and police to combat counterfeit skimming. It has helped destroy several major counterfeiting rings run by organised criminals.

The FIB is developing further its role as a leading centre for exchange of information and intelligence between police and the banks on all types of card fraud. The FIB will work closely with the dedicated cheque and plastic crime unit.

Helping retailers fight fraud

Training and rewarding retail staff for stopping fraud

A major retailer training initiative, run on behalf of the UK banking industry in close collaboration with retailers, police and organisations including Crimestoppers, is educating retail staff how to identify and prevent card fraud.

APACS' Spot & Stop Card Fraud programme has helped reduce fraud losses significantly. Last year the annual fraud loss growth rate in the eight cities that received targeted training was reduced by 47 per cent.

For 2002 the initiative is concentrating on a new group of fraud-prone areas, targeting retailers in West London, Manchester, Glasgow, Harrow, Uxbridge, Ilford, Romford, Enfield, Dartford, Kingston-upon-Thames, Twickenham, Slough and Bradford.

The initiative is part of a wider, ongoing retailer education programme that includes producing a range of free publications as well as co-ordinating an annual campaign that highlights a current fraud issue to retailers and cardholders.

UK card issuers run a retailer reward scheme that paid out more than £10 million in 2001 to staff who retained cards that were being used fraudulently.

System to reduce card-not-present fraud

Fighting fraud on telephone, mail order and internet transactions

To combat the rapid rise in card-not-present fraud, the UK card industry has developed a system that allows merchants who accept transactions via the phone, mail order or the internet to verify the billing address of a cardholder and cross-check a card security code. Cardholders are asked to provide their full statement address and the last three- or four-digit number – known as the card security code – printed on or just below the signature panel on their card.

In most frauds of this type, a card criminal only has access to a stolen receipt containing limited card details, so they would not be able to provide the real cardholder's address or the code on the back of the card.

The extra data checks will provide additional information to the merchant to help them assess potential fraud risks and decide whether to proceed with the transaction.

The international card schemes are also rolling out new security measures to prevent criminals using other people's card details on internet transactions (see page 18).

Under the umbrella of APACS, a cross-sector working group – involving banks, retailers, fraud prevention system providers 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

Banks, building societies and card schemes are continually increasing the sophistication of intelligent detection systems that can identify fraudulent transactions before a card's loss is reported.

If unusual spending is detected, card issuers contact the cardholder to check if the transactions are genuine and, if not, an immediate block can be put on the card. The majority of card issuers already use such systems to considerable success.

Identity theft prevention project

Cross-industry co-operation to fight identity theft

Though identity theft is currently not a significant problem in the UK card industry, it is possible that organised crime gangs will attempt to attack this area in the future, particularly when the chip and PIN system makes its full impact.

The banking industry initiated an identity theft prevention project in early 2002, bringing together a wide range of different industries and organisations that may be impacted by this fraud, such as Government agencies, insurance organisations and law enforcement bodies.

The project is co-ordinating the development of cross-industry strategies and systems with the objective of finding a defence against identity theft criminals that can be applied in all key sectors and geographic areas.

CIFAS – the UK Fraud Avoidance System

Sharing information to stop fraud

CIFAS provides a range of services to enable its 240 member organisations to exchange information towards identifying and preventing fraud, including that relating to plastic cards. CIFAS' main emphasis is on identity, application and first party fraud. See www.cifas.org.uk for more information.

In 2001 CIFAS members investigated over 58,000 confirmed fraud cases involving plastic cards.

Lower floor limits

On-line checks to ensure cards are not reported as being used fraudulently

Most retail outlets have a floor limit – an amount above which they will seek authorisation from the card issuer before completing a transaction. Retailers have been incentivised to introduce lower floor limits since the early 1990s and the number of authorised transactions has now increased from 10 per cent to around 70 per cent.

Industry Hot Card File (IHCF)

Checking every card transaction for cards being used fraudulently

Many retailers subscribe to this electronic file which 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 five million missing cards and is used by more than 80,000 participating retailers in the UK. More than 335,000 cases of attempted fraud were prevented by this system in 2001.

The payments industry is actively encouraging extension of its use both in the UK and abroad, where it will help to combat cross-border fraud.

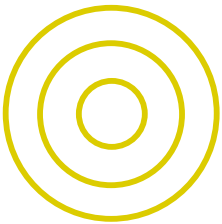
Receiving cards securely

Secure delivery methods for new cards

To minimise the risk of a new card being stolen before the cardholder receives it, the banking industry works in close partnership with the Post Office and courier services to continually enhance secure delivery methods.

'The banking industry, police and retailers, with support from the Home Office, will continue to work together to beat the UK's card fraud problem. The roll-out of the chip and PIN system and the formation of a dedicated police unit to combat counterfeit card fraud are extremely positive moves in our commitment to drive down card crime.'

– David Cooper,
Chairman of APACS' Plastic Fraud Prevention Forum



Advice for cardholders

Educating cardholders
Card Watch aims to increase awareness among cardholders of what they can do to prevent fraudulent use of their cards.

Cardholder liability
While UK codes and legislation makes cardholders potentially liable for the first £50 of fraudulent losses before their card is reported lost or stolen, in practice the bank or building society will usually refund the full amount lost. If a cardholder's details are compromised as in counterfeit skimming or card-not-present frauds, there is no liability.

Visit the Card Watch website at www.cardwatch.org.uk for more information on how to prevent card fraud and what to do if you become a victim.

Card Watch offers cardholders the following advice:

Top tips

1. Guard your cards. Don't let them out of your sight when making a transaction and report lost and stolen cards, or suspected fraudulent use of your card account, to your bank or building society immediately.
2. Don't carelessly discard receipts from card transactions. If possible, shred any documents that contain information relating to your financial affairs.
3. Check your receipts against your statements carefully. If you find an unfamiliar transaction, contact your card issuer immediately.
4. Never write down your PIN and never disclose it to anyone, even if they claim to be from your bank or the police.
5. When using a cash machine, be wary of anyone trying to watch you enter your PIN and do not allow yourself to be distracted.

Internet fraud

Most internet fraud involves using card details fraudulently obtained in the real world to make card-not-present transactions in the virtual world. Card-not-present fraud on internet transactions is low at around £12 million, accounting for three per cent of all card fraud losses.

In April 2001 the UK banking industry began rolling out a cardholder address and card security code checking system to make card-not-present transactions – including those over the internet – more secure (see page 13).

Security of cardholder information

The incidence of hackers stealing cardholder data from websites is very low compared to other ways criminals access card details. To protect data, the international card schemes have stringent criteria to help retailers protect their websites.

The international card schemes are rolling out new security measures to prevent criminals using other people's card details on internet transactions. Visa's system is called 3D Secure and MasterCard's is Secure Payment Application (SPA). Further details can be obtained from these organisations' websites (see page 29).

Chip cards used with PINs have the potential to play a pivotal role in providing the base for secure transaction technology in the future, when it is possible that chip readers and PIN pads attached to computers, digital TVs or phones will help protect these types of transactions against fraud.

Ten-point checklist for internet transactions

The vast majority of businesses operating on the internet are honest and legitimate organisations. Cardholders need only to follow the guidelines given below to make e-commerce no more risky than buying by mail order or over the telephone.

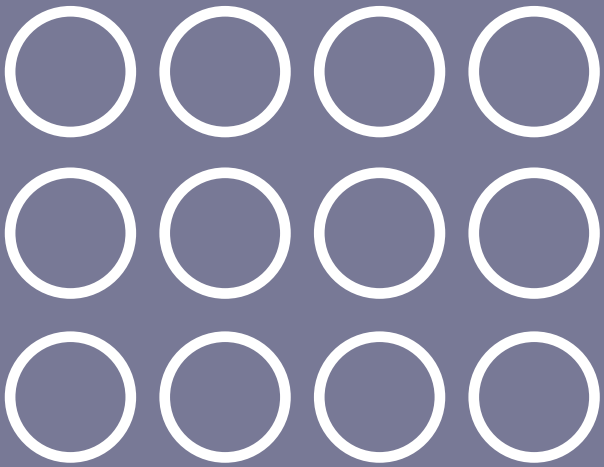
APACS recommends the following ten-point checklist when shopping on the internet.

1. Know who you are dealing with – get the seller's phone number (not a mobile) and postal address (not a post office box).
2. Never disclose your PIN to anyone and never send it over the internet.
3. Ensure that the locked padlock or unbroken key symbol is shown 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.
4. 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.
5. 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.
6. Click on the security icon to ensure that the retailer has an encryption certificate. This should explain the type and extent of security and encryption it uses.
7. 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.
8. Print out your order and keep copies of the retailer's terms and

conditions and returns policy. 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.

9 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.

10 If you have any doubts about giving your card details, find another method of payment.



Card facts and figures

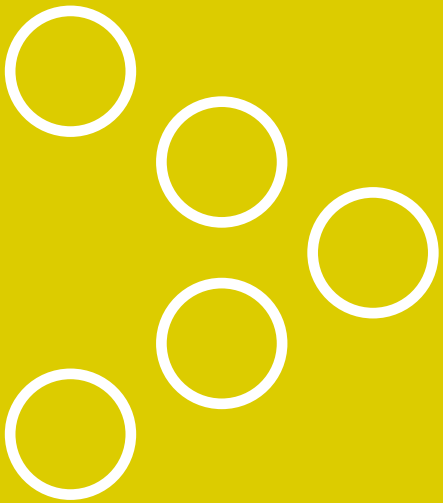
- Credit cards were first issued in the UK in 1966 and debit cards in 1987. Since then, card usage has grown every year: in the past five years the number of cards in issue has grown by 32 per cent. Today there are more than 42 million cardholders in Britain and almost 137 million plastic cards including credit, charge, debit, cash (ATM only) and cheque guarantee cards
- 89 per cent of adults hold one or more plastic cards
- 56 per cent of adults hold a credit/charge card
- 84 per cent of adults hold a debit card
- Credit and debit card purchase volumes are expected to more than double in the next ten years
- The first ATMs were introduced in 1967. The early machines had limited functions, dispensing fixed amounts of cash in exchange for tokens. It was only in the mid-1970s that magnetic stripe cards were used to withdraw cash
- There are 36,700 ATMs in the UK
- On an average day there are around 6 million cash withdrawals from ATMs (about 2.2 billion in total during 2001)
- The average ATM withdrawal is £58
- The average ATM user visits an ATM once a week
- The average annual spend per credit card is approximately £1,400
- The average purchase on a credit card at a retail outlet is around £54
- Nearly 6.6 billion transactions were made with plastic in 2001
- Around £188 billion was spent by UK cardholders in UK card-based retail transactions in 2001
- In 2001, the average total loss per lost or stolen credit or debit card used fraudulently was £448
- £411.4 million was lost to card fraud last year
- More than 69 per cent of all fraudulent card use in the UK takes place at the retail point-of-sale

The major players

The major players in card fraud prevention are the banks, retailers and police. Their continuing efforts focus on developing tougher measures that are both effective at combating fraud and realistic from an operational point of view.

Leading the fight against fraud is APACS' Plastic Fraud Prevention Forum (PFPF), comprising representatives of all the major card issuers in the UK and the card schemes including Visa and Europay/MasterCard. Its role is to develop and implement strategies to prevent card fraud.

Card Watch is APACS' public awareness campaign. For more information see www.cardwatch.org.uk.



Useful contacts

APACS
Switchboard: 020 7711 6200
Public Affairs: 020 7711 6234
publicaffairs@apacs.org.uk
Card Services: 020 7711 6280
melanie.hubbard@apacs.org.uk
mark.bowerman@apacs.org.uk
www.apacs.org.uk

APACS MEMBER BANK AND BUILDING SOCIETY CONTACTS

Abbey National
Switchboard: 0870 607 6000
Press office: 020 7612 4979
Press office fax: 020 7612 4738
christina.mills@abbeynational.co.uk
www.abbeynational.co.uk

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

Useful contacts (cont)

Bank of Scotland (HBoS)
Switchboard: 0131 442 7777
Press office: 0131 243 7077
Press office fax: 0131 243 7082
alistair_ross@bankofscotland.co.uk

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

Barclays Bank
Retail Financial Services Communications
Switchboard: 020 7699 5000
Press office: 020 7699 2387
Press office fax: 020 7699 3644
louise.footner@barclays.co.uk
www.barclays.co.uk

Capital One
Switchboard: 0115 843 3300
Press office: 0115 843 3174
Press office fax: 0115 843 3388
richard.holmes@capitalone.com
www.capitalone.co.uk

Citigroup
Switchboard: 020 7500 5000
Press office: 020 7986 5602
Press office fax: 020 7986 5610
stephen.goldman@ssmb.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 5522
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.a.cooper@coutts.com
anita.saunders@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

Halifax (HBoS)
Switchboard: 01422 333 333
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 892 411
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 7260 8206
Press office fax: 020 7260 8215
Out-of-hours pager numbers for duty press officers: 0941 105821/105914
pressoffice@hsbc.com
www.hsbc.com

Lloyds TSB Bank
Switchboard: 020 7626 1500
Press office: 020 7356 2493
Press office fax: 020 7356 1369/2494
mary.walsh@lloydstsb.co.uk
www.lloydstsb.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

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

Nationwide
Switchboard: 01793 655 000
Press office: 01793 655 198
Press office fax: 01793 655 045
pressoffice@nationwide.co.uk
www.nationwide.co.uk

Useful contacts (cont)

Natwest Group
Switchboard: 020 7920 5555
Retail bank press office: 020 7920 5029
Press office fax: 020 7920 5514
ronan.kelleher@rbs.co.uk
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 7920 5847
Press office fax: 020 7920 1862
jayne.goodwins-miller@rbs.co.uk
www.rbs.co.uk

Woolwich
Retail press office: 020 7699 4077
Retail press office fax: 020 7699 3644
perry.jones@woolwich.co.uk
www.woolwich.co.uk

CARD SCHEME CONTACTS

Visa International
Switchboard: 020 7937 8111
Press office fax: 020 7795 5560
barderr@visa.com
www.visa.com

Mastercard/Europay International (Brussels)
Press office: 00 32 2 352 5647
Press office fax: 00 32 2 352 5732
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 7233 0873
jacqueline.a.goozee@aexp.com
www.americanexpress.com

Diners Club
Press office: 020 7986 5602
Press office fax: 020 7986 5610
stephen.goldman@ssmb.com

Publications

All available from: APACS Public Affairs request line, 020 7711 6359 or publicaffairs@apacs.org.uk

Plastic Card Review (£50 charge may apply)
An annual publication providing a comprehensive analysis of trends in plastic card use in the UK.

Fraud in Focus
An annual publication offering an overview of fraud trends and current fraud prevention initiatives (available in pdf format from www.cardwatch.org.uk).

Spot & Stop Card Fraud pack
A collection of fraud prevention literature for retail point-of-sale staff, including a four-step guide to spot and stop card fraud designed to be kept at the sales counter. Free packs can be ordered from the Card Watch Information Office on 08705 500 005, or visit www.cardwatch.org.uk.

Glossary

Acquirer (merchant acquirer)

The bank or other financial institution which has a contractual agreement with a merchant. The acquirer processes debit and credit card transactions it receives, reimbursing the merchant for the amount of the sale and levying a service charge for the service.

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

Automated Teller Machine (ATM)
A computerised self-service device permitting the holder of an appropriate card and PIN to withdraw cash from their account and access other banking services. Also known as a cash machine, cash dispenser or hole-in-the-wall machine.

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

Card Authentication Method (CAM)
The means by which a plastic card is determined genuine and not counterfeit. The chip card provides the best CAM available.

Card issuer
The bank, building society or other financial institution that issued the card and which has a contractual relationship with the cardholder.

Card-not-present (CNP)
A transaction where the merchant does not have physical access to the card (e.g. through telephone, mail order or internet transactions).

Card schemes
Organisations which manage and control the operation and clearing of transactions. Banks and building societies must be members of the appropriate schemes to issue cards and acquire card transactions. Examples of schemes are: MasterCard/Europay, Visa, Switch, American Express, Diners Club International.

Card Security Code
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.

Cardholder Verification Method (CVM)
The means by which the presenter of the card may be identified as genuine, for example a signature or PIN.

Chip card
A plastic card containing a microchip which has highly secure memory and processing capabilities. These can be recognised by the gold or silver coloured contact plate on the front of the card. Chip cards are also known as integrated circuit cards (ICCs) or smart cards.

CIFAS – The UK Fraud Avoidance System
CIFAS is an information exchange that helps its wide range of member organisations identify different types of fraud, including that on plastic cards.

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

Cross-border fraud
Fraud perpetrated on a plastic card, or using a card number, in a country other than the country of issue.

Electronic commerce (e-commerce)
Transactions which 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, this is a pre-paid card that contains electronic value exchanged for goods and services. It can be disposable or reloadable.

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.

Glossary (cont)

Fraud Intelligence Bureau (FIB)
A rapid response unit based at APACS that shares information between the banks and police to combat counterfeit fraud.

Industry Hot Card File (IHCF)
Computerised list of lost or stolen cards, for use by merchants.

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.

Skimming
The most prevalent form of counterfeit fraud whereby a card's magnetic stripe details are electronically copied and put onto another card.