



APACS

2002 **Fraud in Focus**

An update on measures to prevent plastic card fraud



Contents

- 1 A revolutionary move to fight fraud
- 2 Card fraud – the facts
- 4 Types of fraud
- 6 Preventing fraud with chip cards and PINs
- 7 Further fraud prevention initiatives
- 10 Fraud and the internet
- 11 Summary of UK industry major fraud prevention initiatives
- 12 The major players
- 13 Information sharing

A revolutionary move to fight fraud

Fraud prevention is a top priority for the UK card industry, with 2001 losses up 30 per cent on the previous year to £411.4 million. The steep rise in card fraud over the last few years has been caused by high levels of organised card crime alongside increases in the number and usage of payment cards.

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

The chip cards now being introduced in the UK – already there are more than 25 million – meet the first of these objectives by ensuring that a card is not a counterfeit. This is because the microchip holds the card data so securely that it cannot feasibly be copied or altered.

To meet the second objective, the banking industry has committed to ensuring that by 2005 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. By using the security of chip cards, the new system is expected to more than halve predicted card fraud losses.

Against a backdrop of shared concern between the banks, retailers, police and the Home Office, card fraud prevention efforts continue on a range of other initiatives to bridge the gap until the longer term benefits associated with chip cards can be realised.

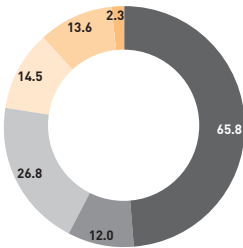
David Cooper

Chairman of the APACS Plastic Fraud Prevention Forum

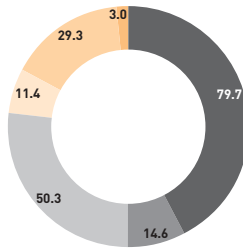
Card fraud – the facts

The UK has seen card fraud losses rise significantly in recent years, reaching £411.4 million in 2001. This represents an increase of 30 per cent on the figure of £317 million* reached in 2000.

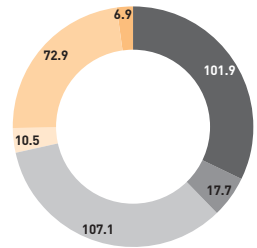
Rises in counterfeit and fraud involving transactions made via the phone, mail or internet were the main reasons behind the increase. Criminals – many of them involved in organised gangs – have increasingly adopted these fraud methods to take advantage of technology and new payment channels.



1998: £135 million

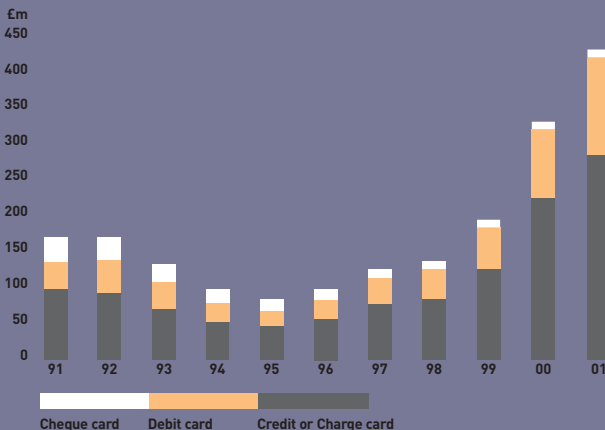


1999: £188.4 million



2000: £317 million

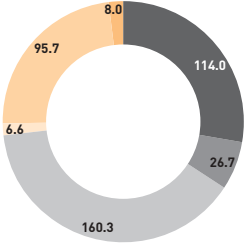
Graph of fraud losses over last decade



* Original 2000 figure of £292.6 million published during 2001 by APACS has been adjusted from net/gross to a gross figure of £317.0 million to allow a direct comparison with the 2001 figure.

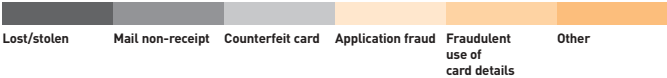
Over 33 per cent of fraud losses on UK-issued cards occur overseas. Most of these losses take place in the United States (19% of total cross-border losses in 2001), France (17%) and Spain (16%). Cross-border fraud losses increased by 34 per cent on the previous year's figure, costing the industry £138.4 million.

The graph shows the pattern in total fraud losses over the last decade and the year-on-year percentage growths.



2001: £411.4 million

The pie charts show that the proportion of fraud on lost or stolen cards is decreasing. Counterfeit fraud and the fraudulent use of card details (card-not-present fraud) are increasing significantly.



The pattern of fraud shows a steep reduction in losses from the early to mid-1990s, as a result of a range of partnership prevention initiatives, and then acceleration to 2002 as criminals adapted their methods. Large growths are seen in counterfeit and card-not-present fraud.

To put the fraud increases in context, it must be remembered that card usage and the number of cards in issue continues to grow strongly in the UK. As a consequence, fraud losses against turnover, at 0.183 per cent in 2001, were just over half the 1991 peak level of 0.33 per cent.

Types of fraud

Counterfeit

Counterfeit losses hit £160.3 million in 2001, an increase of 50 per cent on the 2000 figure. Counterfeit is the fastest growing and biggest loss type for card fraud because international organised criminals tend to use it on a large scale, generating money to fund other serious crimes.

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 then altered or recoded.

The most common form of counterfeiting is called skimming, which involves a criminal copying the magnetic stripe on a credit or debit card by swiping it through a small card reader. The card data is then used to make counterfeit cards. Skimming is usually carried out by corrupt staff working in bars, restaurants and petrol stations.

Sometimes the details obtained by skimming are used to carry out fraudulent transactions via the phone, mail order or internet (see below).

Fraudulent use of card details (card-not-present fraud)

This crime involves using fraudulently-obtained card details to make a purchase. Usually the details are taken from a discarded receipt or copied from a card without the owner's knowledge. Most of this fraud occurs through telephone or mail order, and less frequently through the internet (see Fraud and the internet section).

Losses resulting from fraudulent use of card details increased by 31 per cent to cost £95.7 million in 2001.

Fraud on lost or stolen cards

Most fraud on lost or stolen cards takes place at retail outlets before the cardholder has reported the loss. In other cases, the details from lost and stolen cards are used to make card-not-present transactions.

Fraud on lost or stolen cards cost the banking industry £114.0 million in 2001, rising 12 per cent from 2000. This type of fraud accounted for 28 per cent of total losses in 2001.

Mail non-receipt fraud

The number of newly-issued plastic cards stolen before cardholders receive them peaked in 1991 when fraud on such cards cost the industry £33 million. At this point the banking industry formed an ongoing partnership with the Post Office to monitor and control card distribution. This work drove down the cost of this type of fraud significantly and has kept it low ever since.

Despite this remaining a small category of fraud, there was a significant increase in 2001 of 51 per cent to £26.7 million. This illustrates how criminals look for alternative areas to exploit as fraud prevention systems drive them away from their usual methods.

Identity theft

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

Total identity theft cost an estimated £12 million in 2001, made up of £6.6 million for application fraud and an estimated £5 million for account take-over.

Application fraud

Application fraud occurs when criminals use stolen or false documents to open an account. Criminals may try to steal documents like utility bills and bank statements to build up useable information. Alternatively, they may use counterfeited documents for identification purposes.

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.

ATM (automated teller machine) fraud

ATM fraud is not a type of fraud but the place where it occurs, usually with lost and stolen cards. Many 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 and then steal the card using distraction techniques or pickpocketing.

ATM fraud that involves card-trapping devices is also on the rise. The device snares 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 and the card and withdraws cash.

Fraud at ATMs in the UK cost the banking industry £21.2 million in 2001, representing 5.2 per cent of total fraud losses.

Preventing fraud with chip cards and PINs

Very high levels of fraud prevention can be achieved with the use of PINs with chip cards. This system satisfies the two fundamental objectives of card fraud prevention – helping to prove that the card is not a counterfeit and that the cardholder is the genuine owner.

With the aim of drastically reducing card fraud losses, over the next two to three years all 100 million UK debit and credit cards will be reissued with embedded microchips which have been programmed with the capability of identifying cardholders using a PIN.

The UK chip offers global interoperability as it meets specifications laid down by the international card schemes Europay/MasterCard and Visa (EMV). Most European countries are about to issue cards to the same specification, and over time there will be increasing use of these cards around the world.

Major investment

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

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

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

Benefits of chip cards

Initially, the major advantage of chip cards is the increased security they provide against counterfeit. Chip technology uses sophisticated processing to identify genuine cards and make counterfeiting extremely difficult and hugely expensive. The sophistication of the chip makes it able to support a highly secure PIN identification system.

Additionally, chip cards have the ability to support 'add on' services such as retailer loyalty schemes or electronic purses and provide opportunities for secure new services in the fields of electronic commerce and home banking.

What about iris scanning and other biometric methods?

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 verification have been suggested as possibilities. However, such technology is unlikely to be sufficiently reliable to meet the requirements of the UK card industry within the next ten years.

Further fraud prevention initiatives

Chip security systems will continue to be reviewed and updated regularly, and the UK card industry maintains a multi-layered approach to security so that it is not reliant on any single technique. To ensure a broad attack against card criminals, a range of prevention initiatives continues to be developed and enhanced in partnership with retailers, police and the Government.

Counterfeit card fraud

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 that helps 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 like drug trading. If the pilot proves successful, the unit has the potential to become permanent.

The 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)

Based at APACS, the FIB shares information and intelligence between the banking industry and police to identify retail outlets where cards have been skimmed. It has helped destroy several major counterfeiting rings run by organised criminals. Its role continues to expand as a leading centre for exchange of information between police and the banks on all types of card fraud.

The FIB works hand-in-hand with the dedicated police unit, providing intelligence from the card industry to facilitate investigations.

Card-not-present fraud prevention

Cardholder address and card security code checking in the medium term

In April 2001, the UK banking industry began rolling out a system to make card-not-present transactions more secure. The automated address and card security code checking system allows merchants who accept transactions via the phone, mail order or the internet to verify the billing address of cardholders and cross-check coded digits printed on the signature strip of cards.

The system has the ability to make a significant impact as, in the majority of cases, a criminal would try to use a discarded receipt to make a transaction and so would not be able to provide the real cardholder's address or the code on the back of the card.

Further fraud prevention initiatives (cont)

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.

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.

Visa and MasterCard are working on new internet security measures that would enable companies to confirm the identity of the consumer online.

Helping retailers fight fraud

Retailer education and reward programmes

A major new retailer training initiative, run on behalf of the UK banking industry in close collaboration with retailers and police, is teaching retail staff to identify and prevent card fraud attempts.

The Spot & Stop Card Fraud programme is targeting retailers in the UK's top fraud-prone areas and has helped reduce fraud losses significantly. In 2001 the fraud loss growth rate in the eight cities that received targeted training was slowed by 47 per cent.

This initiative is part of a wider, ongoing retailer education programme that includes providing a range of free materials as well as running an annual campaign for retailers and cardholders to raise awareness of a topical fraud issue.

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

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 or misuse 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.

Cross-industry co-operation to fight identity fraud

Though identity fraud 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 fraud prevention project in early 2002, bringing together a wide range of different industries and organisations that may be impacted by identity 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 fraud criminals that can be applied in all key sectors and geographic areas.

CIFAS – The UK's Fraud Prevention Service

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

Online checks to ensure cards have not been reported lost or stolen

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

The Industry Hot Card File

Checking every card transaction to ensure cards are not reported as lost or stolen

Many retailers subscribe to this electronic file which distributes data on lost and 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.

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.

Fraud and the internet

Most internet fraud involves criminals using card details fraudulently obtained in the real world to make card-not-present transactions in the virtual world. Currently such fraud on internet transactions is low – estimated losses remain modest at around £12 million, around three per cent of total 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 Further fraud prevention initiatives).

Security of cardholder information

Although the incidence of hackers stealing cardholder data from websites is very low compared to other ways criminals access card details, there have been some incidents made public by the media. To protect data, the international card schemes have stringent criteria to help retailers safeguard their websites and card information.

For the future

The international card schemes are currently rolling out new security measures to protect internet transactions from fraud. The Visa system is called 3D Secure and MasterCard's is Secure Payment Application (SPA). Further details can be obtained from these organisations' websites.

Chip cards used with PINs may 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.

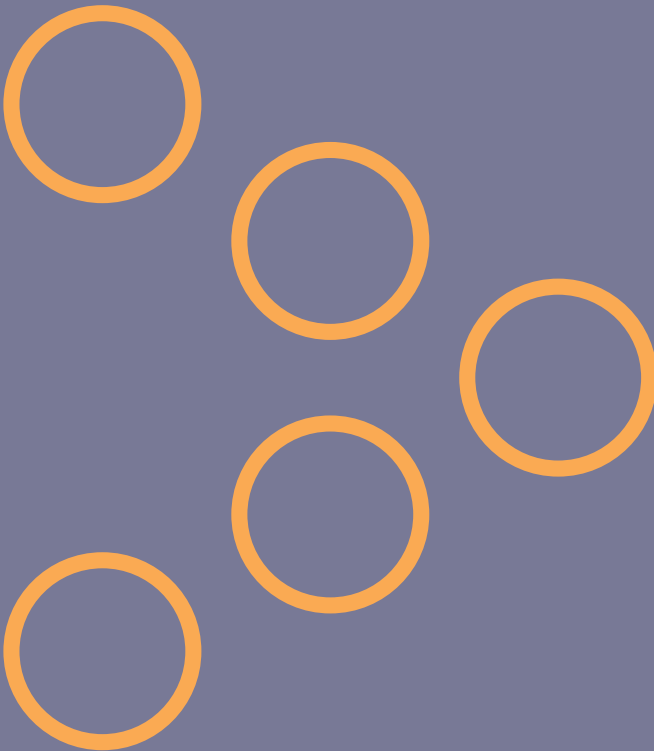
Summary of UK industry major fraud prevention initiatives

- The introduction of chip cards, built to an international standard, to be used with PINs to identify cardholders by 2005.
- A two-year pilot of a dedicated card crime police unit, chiefly funded by the banking industry, to focus on organised card criminals.
- Roll-out of an address and security code checking system to reduce card-not-present fraud and consideration of further enhancements to security of such transactions.
- A major training and education programme for retail staff, Spot & Stop Card Fraud, was launched in 2001 and continues to be expanded in 2002.
- Giving rewards to retail staff who stop a card being used fraudulently (in excess of £10 million was paid in rewards in 2001).
- The use of intelligent computer systems that monitor cardholder accounts to spot fraud at an early stage.
- Developing a cross-industry project to prevent identity fraud.
- Increasing the number of transactions authorised at retailers (from around 10% in the early 1990s to 70% today).
- The use of hot card files carrying details of lost and stolen cards.
- Implementation of a wide range of secure methods for delivering cards.
- Maintaining a close partnership between banks, retailers and police.
- Developing Visa's 3D Secure and MasterCard's Secure Payment Application systems to combat fraud conducted over the internet.

The major players

Fighting card fraud is a partnership effort between the banking industry, police, retailers and the major card schemes: Europay/MasterCard, Visa, American Express, Switch and Diners Club.

The APACS Plastic Fraud Prevention Forum comprises representatives of all the major card issuers in the UK and the card schemes. Card Watch is PFPF's fraud prevention awareness programme for retailers and the card-holding public.



Information sharing

The following are available from the APACS Public Affairs request line on 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 over the last seven years.

Card Fraud – The Facts

A booklet on card fraud for journalists and others.

The following are available at no cost to the appropriate audience and can be downloaded or ordered at www.cardwatch.org.uk.

Spot and Stop Card Fraud

An easy-to-use guide for retailers which goes through the four key procedures for spotting and stopping card fraud.

Card Force

Newsletter on card fraud prevention for police and retail security departments.

Counter Attack

Newsletter with fraud prevention advice for retail staff.

For further information about card fraud prevention please contact cardwatch@apacs.org.uk, visit www.cardwatch.org.uk or contact APACS Card Services on 020 7711 6356.