Fraud
The Facts 2007

The definitive overview of payment industry fraud and measures to prevent it

APACS

APACS is the trade body that gives banks, building societies and card issuers a forum where they can work together on non-competitive issues. In a nutshell we help manage the way that businesses and individuals in the UK move their money around – this covers cash, credit and debit cards, cheques and automated payments such as direct debits, salary payments and online/phone transactions. We also champion the fight against banking fraud and are the people who have been working to give consumers greater card fraud protection by introducing chip and PIN. Twice a year we publish figures on banking fraud losses.

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

"For two consecutive years fraud losses on UK-issued cards have decreased. This is testament to the overwhelming success of chip and PIN – especially in the high street where losses have fallen by 67% in the past two years.

However, as detailed in this booklet, some categories of fraud are still increasing. The banking industry remains fully committed to containing and reducing all areas of fraud. The introduction of chip and PIN in the UK and the creation of the Dedicated Cheque and Plastic Crime Unit are evidence of this. As well as reducing fraud, maintaining customer confidence in the security of the UK's payment systems is a key requirement and we will continue to work with law enforcement, the retail sector, the Home Office and organisations such as MasterCard, Visa and Crimestoppers to help achieve these ends.

For the first time this booklet also contains information on payment, lending and insider fraud as we look to increase transparency and explain more fully the different fraud threats that the industry faces."

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

Plastic card fraud

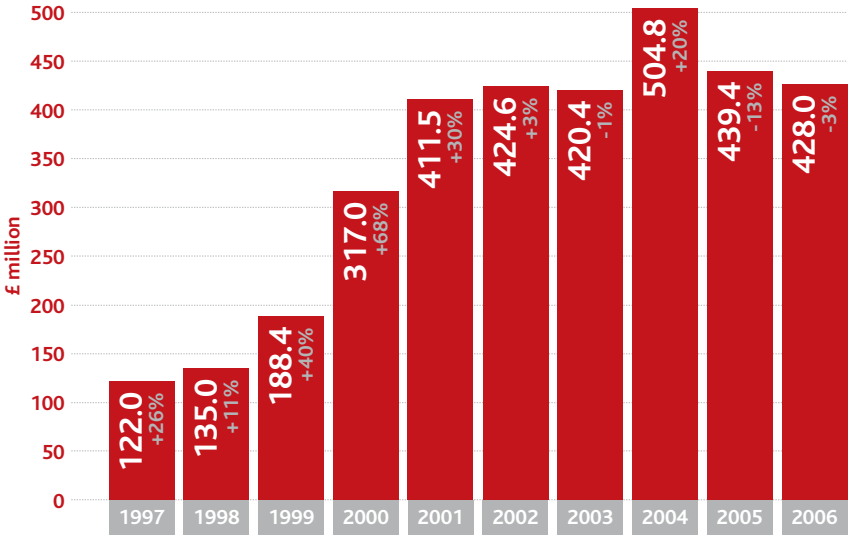
4 Plastic card fraud losses on UK-issued cards 1997-2006

6 Overview of types of plastic card fraud

26 Industry measures to prevent plastic card fraud

Plastic card fraud losses on UK-issued cards 1997-2006

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



Annual plastic card fraud losses on UK-issued cards 1997-2006

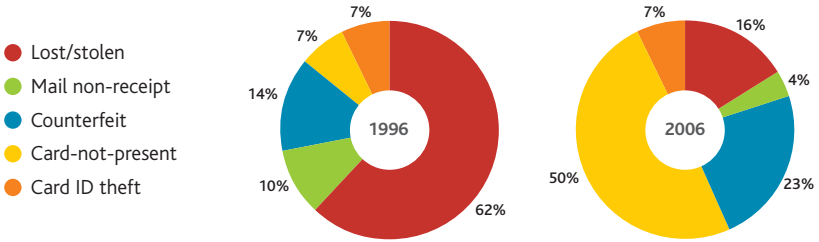
All figures in £ millions

Fraud type	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Card-not-present	10.0	13.6	29.3	72.9	95.7	110.1	122.1	150.8	183.2	212.6
Counterfeit	20.3	26.8	50.3	107.1	160.4	148.5	110.6	129.7	96.8	99.6
Lost/stolen	66.2	65.8	79.7	101.9	114.0	108.3	112.4	114.5	89.0	68.4
Mail non-receipt	12.5	12.0	14.6	17.7	26.8	37.1	45.1	72.9	40.0	15.4
Card ID theft	13.1	16.8	14.4	17.4	14.6	20.6	30.2	36.9	30.5	31.9
Total	122.0	135.0	188.4	317.0	411.5	424.6	420.4	504.8	439.4	428.0
Contained within this total										
UK retailer (face-to-face)	72.2	74.8	93.0	139.1	188.9	186.9	177.9	218.8	135.9	72.1
Domestic/international split of total losses										
UK fraud	92.8	100.1	134.1	213.4	273.0	294.4	316.3	412.3	356.6	309.8
Fraud abroad	29.2	34.9	54.2	103.5	138.4	130.2	104.1	92.5	82.8	118.2

Overview of types of plastic card fraud

Whilst card usage and transaction volumes continue to grow, plastic card fraud losses against total turnover – at 0.095% – are significantly less than the 1991 peak level of 0.33%. This fraud-to-turnover ratio fell by 15% from 0.112% in 2005.

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



* *(See table opposite)* Fraud losses in all but two regions (Wales and the North West) reflect what is happening at a national level – card-not-present fraud is rising, but the other fraud types are falling so much that the overall effect leads to a drop in total card fraud.

In Wales and the North West card-not-present fraud losses have increased at a rate greater than the decreases seen in the other fraud types and has caused an overall increase. The card-not-present fraud increases are due to a combination of factors but are most probably influenced by the fact that the head offices of large card-not-present merchants are based in the region. It is not necessarily because card-not-present fraudsters are targeting cardholders in these particular regions.

Plastic card fraud losses in the UK in 2006 on UK-issued cards split by UK region

All figures in £ millions

Region	2004	2005	2006	+/- change
South East	£238.2	£207.3	£180.2	-13%
North West*	£40.2	£33.2	£34.0	+2%
Yorkshire & Humberside	£24.3	£27.3	£25.6	-6%
West Midlands	£24.2	£20.3	£17.7	-13%
East Midlands	£30.8	£23.8	£14.7	-38%
South West	£12.7	£11.3	£9.9	-12%
Scotland	£16.7	£13.9	£9.5	-32%
North East	£8.1	£7.3	£6.3	-14%
East Anglia	£8.7	£6.2	£5.8	-6%
Wales*	£7.3	£5.2	£5.4	+4%
Northern Ireland	£1.1	£0.8	£0.7	-12%
UK total	£412.3	£356.6	£309.8	-13%
Fraud abroad	£92.5	£82.8	£118.2	+43%
Total all UK cards	£504.8	£439.4	£428.0	-3%

Card-not-present or CNP (internet, phone and mail order) fraud: £212.6 million in 2006 (up 16%)

Card-not-present fraud involves stolen card details being used to pay for goods and services over the internet, by phone or by mail order. It is the largest type of card fraud in the UK and has grown by 74% since 2003. Migration to this method of fraud continued throughout 2006, albeit at reducing rates.

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

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

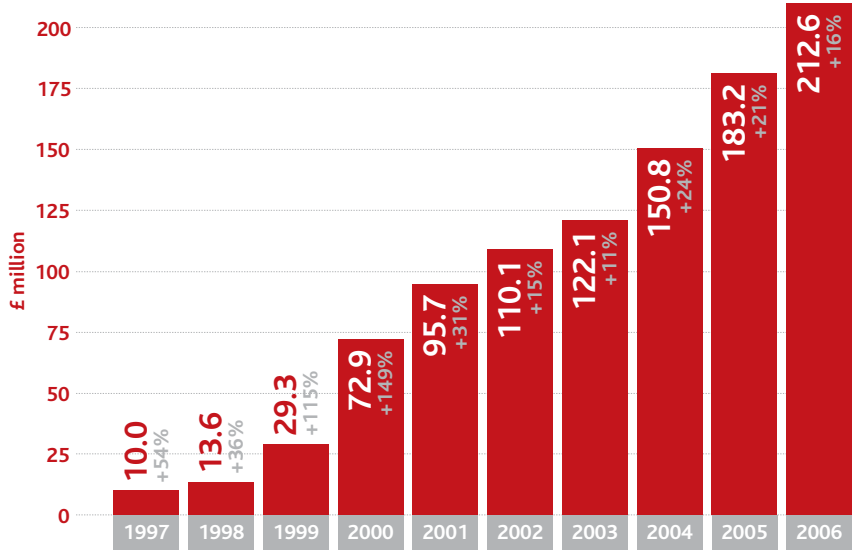
A number of initiatives are available to help businesses protect themselves from card-not-present fraud *(see page 30)*.

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 over the internet, by phone, or mail order. The genuine cardholder may not be aware of this fraud until they check their statement.

Card-not-present fraud losses on UK-issued cards 1997-2006

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



Counterfeit card fraud: £99.6 million in 2006 (up 3%)

Losses in counterfeit fraud have dropped by £60.8 million since 2001 – a fall of 38%. However, a card's magnetic stripe remains a target for fraudsters and most cases of counterfeit card fraud on UK cards involve criminals undertaking old-style fraud where fraudsters copy magnetic stripe details. They then create a fake, magnetic stripe card that can be used overseas in countries that haven't upgraded to chip and PIN. However, as the rest of the world upgrades to chip and PIN, it will become increasingly difficult for fraudsters to use fake magnetic stripe cards overseas.

Total domestic counterfeit card fraud losses have gone down by 32% in the past two years, whereas overseas counterfeit card fraud losses have increased by 16% over the same time period.

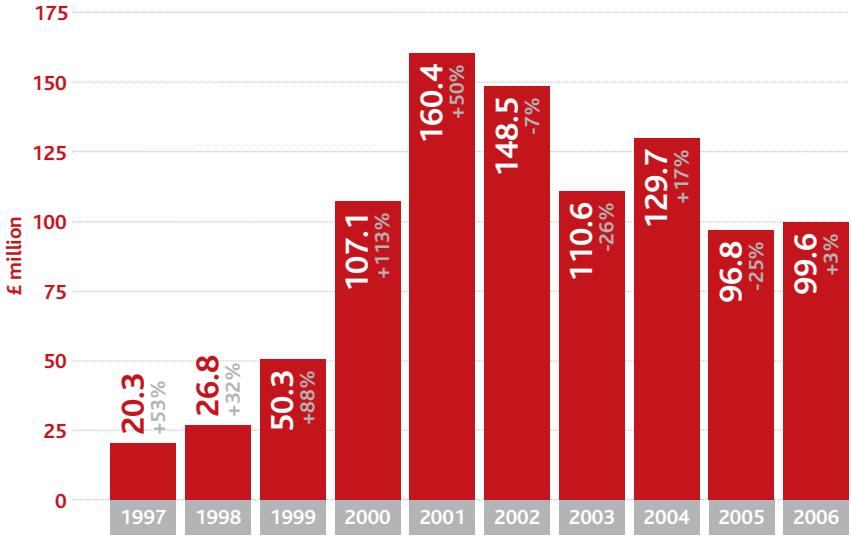
Counterfeit card fraud losses in the UK and abroad 2004-2006

All figures in £ millions

Region	2004	2005	2006	+/- change
Domestic (in the UK)	£105.9	£78.6	£72.1	-8%
Abroad	£23.8	£18.2	£27.5	+51%
Total	£129.7	£96.8	£99.6	+3%

Counterfeit fraud losses on UK-issued cards 1997-2006

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



Lost and stolen card fraud: £68.4 million in 2006 (down 23%)

Thanks to the introduction of chip and PIN this type of card fraud is now at its lowest level for eight years. As well as the proven security benefits of chip and PIN, the banking industry has a number of other initiatives in place to tackle this type of fraud:

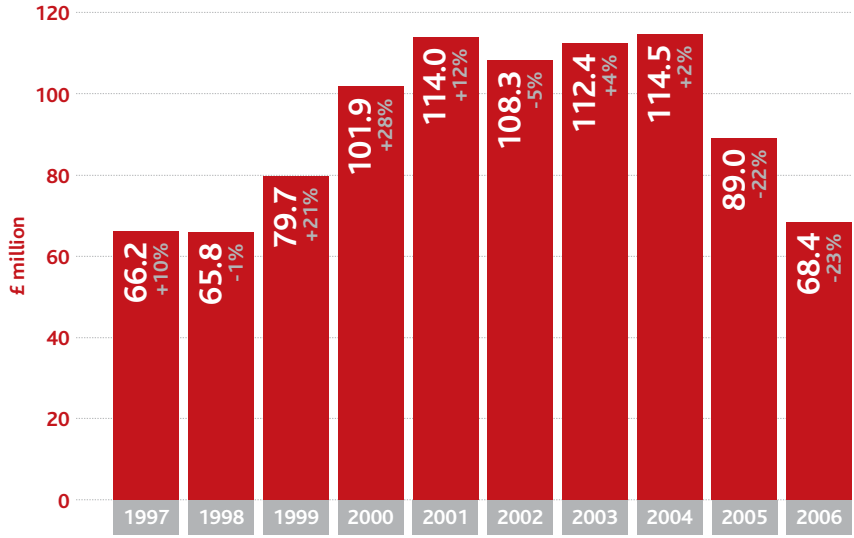
- Intelligent computer systems that card companies use to track customer accounts for unusual spending patterns.
- An Industry Hot Card File *(see page 29)* enables retailers to electronically check whether a card has been reported lost or stolen.
- An APACS-run retailer education programme provides help for shop staff on how to detect stolen and counterfeit cards at the till point. An online version of this retailer-training programme is available at **www.cardwatch.org.uk**.

What is lost and stolen card fraud?

This category covers losses on cards that have been reported by the cardholder as lost or stolen. Most fraud in this category takes place in shops that don't have chip and PIN equipment – as the fraudster does not need a PIN – and before the cardholder has reported the loss of the card.

Lost and stolen fraud losses on UK-issued cards 1997-2006

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



Mail non-receipt fraud: £15.4 million in 2006 (down 62%)

This type of fraud decreased 62% to £15.4 million in 2006, and now represents less than 4% of total card fraud losses. The main reason behind this large decrease is because there are fewer cards and PINs being sent out than in the past few years (approximately 138 million chip and PIN cards were issued between 2004 and 2006). Thus the opportunities for cards to be intercepted before they reach the genuine cardholder are less. Also, when replacement cards are issued, the cardholder already knows the PIN, so the PIN is not sent out. So, if the fraudster intercepts the card, he is unlikely to be able to use the card in the majority of cases.

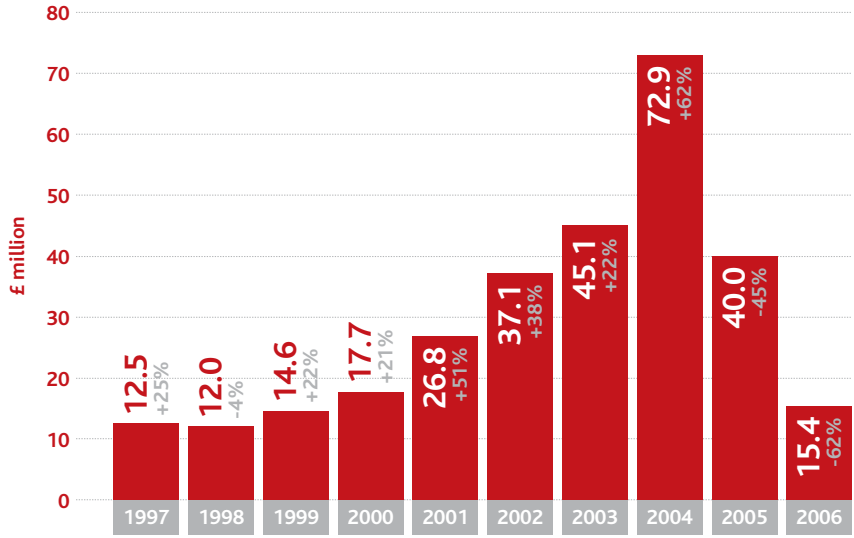
In addition, the banking industry continues to work with Royal Mail and other organisations it uses to deliver its cards to monitor card losses, identify fraud hot spots and take preventative action. Card companies also use secure couriers to deliver to high-risk postcodes or cards may be sent to a customer's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

What is mail non-receipt fraud?

This type of fraud involves cards being stolen in transit – after card companies send them out and before the genuine cardholders receive them. Particularly at risk for this type of fraud are properties with communal letterboxes, such as flats and student halls of residence and people who do not get their mail redirected when they change address.

Mail non-receipt fraud losses on UK-issued cards 1997-2006

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



Card ID theft: £31.9 million in 2006 (up 5%)

Card ID theft can be split into two categories; third party application fraud and account takeover fraud. Third party application card fraud losses in 2006 were £11.9 million, a decrease of 4% from 2005, whilst account takeover card fraud losses in 2006 were £20.0 million, an increase of 11% from the previous year.

Collectively, card ID theft rose by 5% in the past year to £31.9 million and now accounts for just over 7% of overall card fraud losses.

What is card ID theft?

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

Application fraud: £11.9 million in 2006 (down 4%)

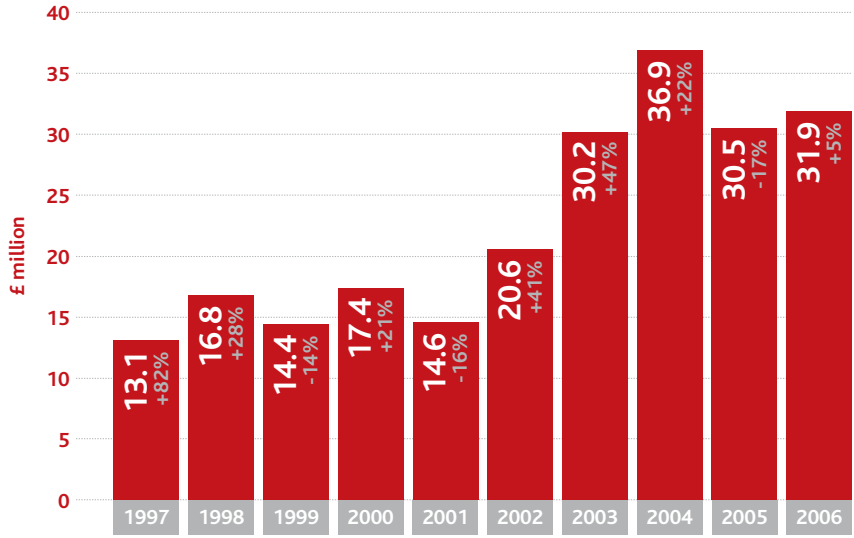
Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeited documents for identification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

Account take-over: £20.0 million in 2006 (up 11%)

Account take-over involves a criminal trying to take over another person's account, first by gathering information about the intended victim, then contacting their bank or credit card issuer whilst masquerading as the genuine cardholder. The criminal will then arrange for funds from the account to be transferred out of the account or will change the address on the account and ask for new or replacement cards to be sent to the changed address.

Card ID theft on UK-issued cards 1997-2006

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



Where does card fraud take place?

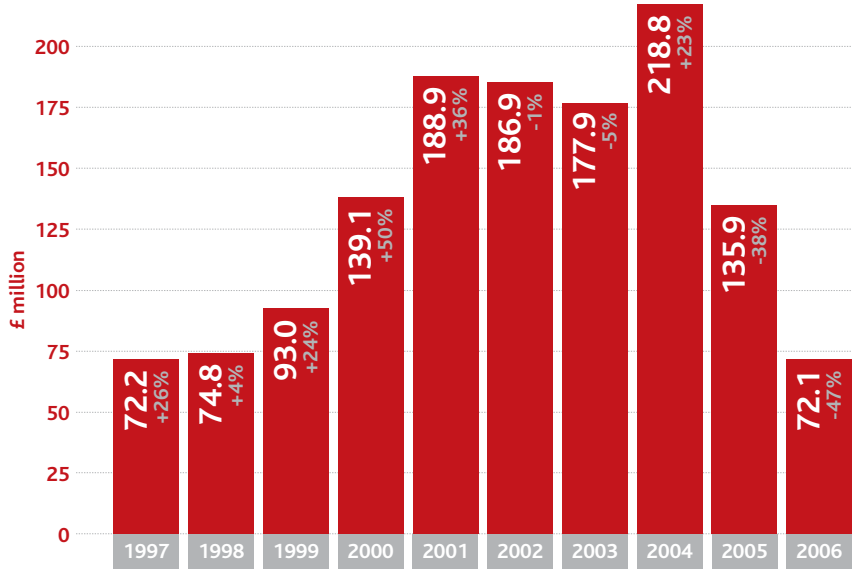
The card fraud landscape is changing due to the continuing success of chip and PIN in the UK. Fraudsters are now looking to target those environments that do not yet use chip and PIN, such as the internet and countries overseas that have not yet upgraded to chip and PIN.

UK retailer (face-to-face) fraud: £72.1m in 2006 (down 47%)

Card fraud losses in the UK high street have declined dramatically since peaking at £218.8 million in 2004. This is directly attributable to the implementation of chip and PIN in the UK, which has seen card fraud in the high street decrease by 67% in just two years.

Card fraud losses at UK retailers 1997-2006

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



Cash machine fraud:
£61.9 million in 2006 (down 6%)

Cash machine fraud is not a type of fraud but describes the location where the fraud occurs. Fraud at cash machines in the UK decreased by 6% last year and accounts for less than 15% of total plastic card fraud losses.

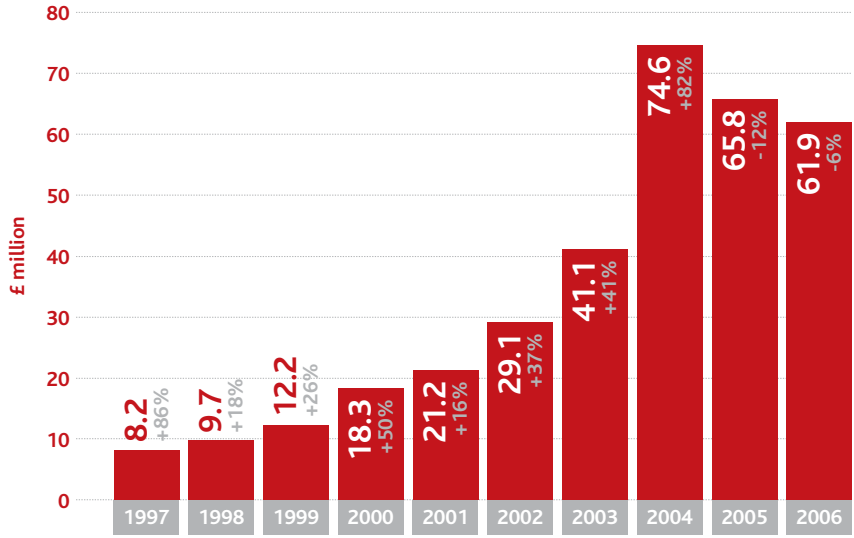
There was a significant increase in this type of fraud during 2003 and 2004 as criminals developed hi-tech ways to copy magnetic stripes and record PINs whilst customers were using cash machines. They would then create fake magnetic stripe cards that would be used with the captured PIN to withdraw money from UK cash machines.

Fraud at this location fell in 2005 and 2006 as the UK moved closer to completing the roll-out of chip and PIN in the UK. All cash machines in the UK have now been upgraded, forcing the fraudsters to use fake magnetic stripe cards in cash machines overseas, in countries that haven't upgraded to chip and PIN.

Unfortunately a large proportion of cash machine crime is still caused by cardholders writing down their PIN and keeping it with their card in their purse or wallet, which is then stolen.

Fraud losses at UK cash machines 1997-2006

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



The three main ways cards and card details are stolen at cash machines are:

- Shoulder surfing – criminals look over a cardholder's shoulder to watch the PIN being entered, then steal the card using distraction techniques or pickpocketing, before using the stolen card and genuine PIN.
- Card-trapping devices – a device, inserted into a cash machine's card slot, retains the card inside the cash machine. The criminal tricks the victim into re-entering the PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.
- Skimming from the magnetic stripe at cash machines – a skimming device is attached to the cash machine to record the electronic details from the magnetic stripe of genuine cards as they are inserted into the cash machine and a miniature camera is hidden overlooking the PIN pad to capture the PIN being entered. Criminals then use the card details to produce a fake magnetic stripe card, which is then used with the genuine PIN to withdraw cash at cash machines overseas that have not upgraded to chip and PIN.

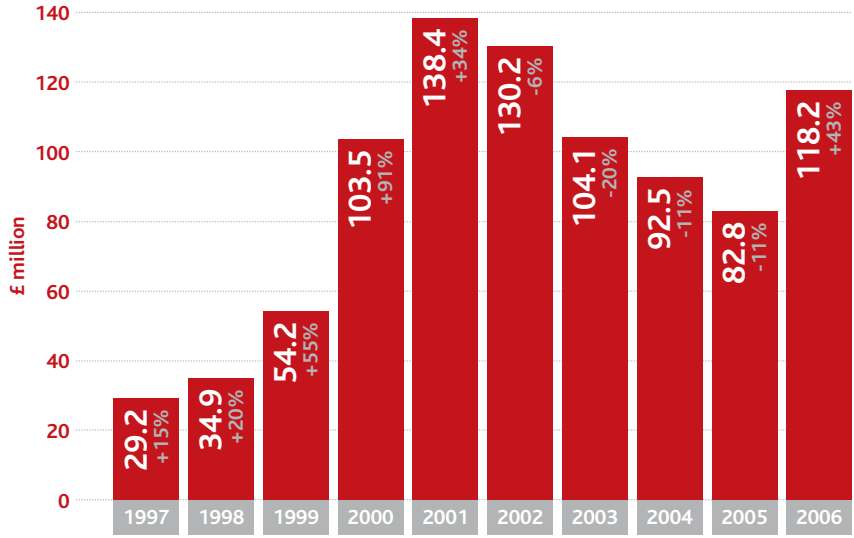
Fraud abroad: £118.2 million in 2006 (up 43%)

The UK is one of the first countries in the world to roll out chip and PIN, which means that fraudsters are increasingly being driven overseas to commit card fraud in those countries yet to upgrade. This has led to an increase in fraud abroad, although the losses are still smaller than they were in 2001 and 2002 (£138.4 million and £130.2 million respectively).

The top three countries for fraud abroad on UK-issued cards remained unchanged from 2005 although this type of fraud is declining markedly in France and Spain as those countries continue their chip and PIN roll-out. Fraud on UK-issued cards in the US increased by 49% to £16.7 million

Fraud committed abroad on UK-issued cards 1997-2006

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



and accounted for 14% of total fraud abroad losses. Fraud on UK-issued cards in France reduced by 35% to £7.5 million (6.3% of the total) and in Spain fraud was down 30% to £6.7 million (5.7% of total). The combined losses of these three countries equated to just 26% of all fraud abroad, which further demonstrates that fraud is migrating to those countries that have not yet rolled out chip and PIN, rather than just those geographically closest to the UK.

Criminals also tend to target popular overseas holiday destinations to lessen their chances of detection by the banks' fraud detection software. However, as the roll out of chip and PIN spreads throughout the world, the concentration of fraud will once again become evident with countries such as the USA likely to be an increasingly targeted region for fraudulent use of UK-issued cards.

Internet/e-commerce fraud on cards: estimated at £154.5 million in 2006 (up 32%)

Internet fraud on cards is part of the card-not-present fraud total of £212.6 million. In 2006 the amount of card-not-present fraud that took place over the internet is estimated at £154.5 million – 73% of total card-not-present fraud losses. This figure has gone up by 32% from 2005, when the internet losses were £117.0 million and accounted for 65% of card-not-present fraud losses.

The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, bin-raiding, data hacking or through unsolicited e-mails or telephone calls. The card details are then used to make fraudulent card-not-present transactions, most commonly via the internet.

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

Industry measures to prevent plastic card fraud

Chip and PIN

Making card transactions safer

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

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

As at January 2007, APACS figures showed that:

- The UK's banks and card companies have issued 138 million chip and PIN cards – representing 97% of the UK's 142 million payment cards.
- Approximately 900,000 shop tills have been upgraded to chip and PIN. This represents 98% of all shop tills in the UK.
- More than 185 chip and PIN transactions take place every second. This compares with 125 every second in January 2006.

While the majority of UK-issued cards are chip and PIN-enabled, some exceptions still exist where people continue to sign:

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

Chip and PIN has made it significantly more difficult for a fraudster to use a lost or stolen card or a counterfeit card in the UK. As the rest of the world upgrades it will make it increasingly difficult for fraudsters to use UK-issued cards abroad.

Dedicated Cheque and Plastic Crime Unit (DCPCU)

A specialist police unit targeting organised criminal gangs

This year marks the 5th anniversary of the DCPCU. In April 2002, APACS, the Association of Chief Police Officers (ACPO) and the Home Office launched the Unit as a two-year pilot to tackle the organised criminal gangs responsible for the majority of cheque and plastic card crime in the UK.

Five years on, the DCPCU is now fully sponsored by the banking industry and has a national remit. During this period the Unit has generated estimated fraud savings of more than £130 million and made 392 arrests with 156 convictions secured.

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

Fraud Intelligence Bureau (FIB)

Exchanging information to fight fraud

The role of the FIB is to distribute information and intelligence between the banking industry, police forces and other law enforcement agencies throughout the UK to combat card fraud. It has helped identify major counterfeiting rings run by organised criminals and provides support to the DCPCU.

Payments Industry & Police Joint Intelligence Unit (PIPJIU)

A joined-up approach to tackle fraud

During 2007, the banking industry plans to merge the industry FIB with the DCPCU intelligence function to form the *Payments Industry & Police Joint Intelligence Unit*, which will have increased funding and a wider remit. The combined intelligence unit will address all types of banking fraud and will not be limited to cheque and plastic card fraud.

CIFAS – the UK's Fraud Prevention Service

Sharing information to stop fraud

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

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

Industry Hot Card File (IHCF)

Checking card transactions for cards being used fraudulently

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

The IHCF contains information on more than 6 million cards reported lost or stolen and over 750,000 cases of attempted fraud have been prevented by this system in the last two years. The IHCF is also being used successfully at motorway tollbooths in France to combat the use of stolen UK cards at road tolls.

The IHCF is increasingly being used by retailers in the card-not-present environment for card checking prior to the dispatch of goods. Extending its use into other fraud prevention initiatives is also under consideration.

Fraud Intelligence Sharing System

Sharing intelligence to tackle fraud

The *Fraud Intelligence Sharing System* (FISS) is a new fraud prevention system, currently under development, that will enable fraud intelligence data to be shared amongst APACS members and law enforcement. The system will provide a secure, pro-active, central intelligence function to support UK retail banking and card institutions. It will also be used by the *Payment Industry & Police Joint Intelligence Unit (see previous page)* and will include plastic and non-plastic fraud data, with cases linked across different products and fraud types.

Fighting card fraud in the retail environment

Training shop staff to stop fraud

Thanks to the introduction of chip and PIN in the UK there has been a significant reduction in card fraud losses on face-to-face transactions in UK shops and businesses, down 47% from 2005 to £72.1 million. Card fraud in the retail environment now represents just 17% of total card fraud losses.

A very small percentage of businesses have yet to upgrade to this new technology and APACS continues to work with these retailers, using its *Spot & Stop Card Fraud* education pack and training programme. Developed in collaboration with retailers, police and organisations including Crimestoppers, it helps retail staff identify counterfeit and stolen plastic cards.

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

Systems to reduce card-not-present (Internet, phone and mail order) fraud

Helping businesses fight CNP fraud

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

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

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

Using chip and PIN to help prevent remote channel fraud

Hand-held card readers that create one-off passcodes

The next stage in making remote channel transactions safer is the implementation of fraud prevention solutions to help tackle fraud in non face-to-face situations (i.e. online banking and internet and telephone shopping). One solution builds upon chip and PIN technology and, for remote shopping, will enhance the online protection already offered by systems such as MasterCard SecureCode and Verified by Visa.

It works via a cardholder inserting their chip and PIN card into a hand-held card reader and entering their PIN. On confirming the PIN entered, the reader generates a unique, one-time only passcode, which the cardholder provides, when prompted, for authentication with their bank. This solution helps to ensure that the person conducting business online or over the phone is the genuine customer and will make these types of transaction even safer. Consumers will start to see the roll-out of these devices during 2007 for use in online banking.

Banks' use of intelligent fraud-detection systems

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

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

Industry measures to prevent card ID theft

Cross-industry co-operation to fight card ID theft

Although card ID theft remains a relatively small proportion of total card fraud losses – just over 7% – prevention measures will remain in place (and will continue to be developed) to combat this type of fraud.

A number of initiatives are currently in place, including:

- Online training available at **www.idfraudpreventiontraining.com**. This initiative has been developed by APACS, the British Bankers' Association and CIFAS, with Home Office backing. It provides best practice guidelines for businesses that could be targeted by identity fraudsters and features an interactive e-learning section to improve the understanding of employees who need to check and verify the identity of customers on a day-to-day basis.
- The Home Office Identity Fraud Steering Committee, consisting of senior representatives from the public and private sectors, including APACS, brings together all those parties with an interest in reducing identity fraud in the UK.
- **www.identitytheft.org.uk** – a consumer-focused website launched by the Home Office with co-operation and assistance from APACS. The website provides the public with practical advice on how best to protect themselves from identity theft and what they should do if they become a victim. This has now been complemented with a range of leaflets and posters for use in public areas including libraries, citizens advice bureaux and bank counters.

Industry measures to prevent cash machine fraud

Multi-layered approach to tackling fraud

Although cash machine fraud losses in the UK have decreased for the past two years, the UK banking industry works continually with cash machine suppliers to enhance technical solutions to prevent cash machine tampering. The industry also works effectively with the police to target the organised criminals behind these types of fraud.

A number of generic initiatives are in place to counter cash machine fraud. These include:

- Use of CCTV to deter fraudulent activity.
- Privacy spaces, which comprise a zoned area marked on the ground in front of the cash machine to enable users to withdraw cash in private. This zone heightens the user's awareness, discourages people from standing close to others when taking money out, and makes it easier to challenge those who cash machine users feel are standing too close.
- Consumer advice on best practice when using a cash machine; this includes co-ordinated use of screen messages designed to raise the awareness of the user at the cash machine.
- Regular inspections of cash machines by cash machine owners for evidence of tampering and unusual attachments.
- Technology upgrades to make cash machines tamper-proof. This includes redesigned card reader surface surrounds in order to make it difficult to attach a skimming device.

Cheque fraud

36 Types of cheque fraud
37 Common cheque fraud scams
38 Industry measures to prevent cheque fraud
40 Liability for cheque fraud

What is cheque fraud?

There are three types of cheque fraud in the UK: counterfeit; forged; and fraudulently altered cheques. In 2006 cheque fraud in the UK amounted to £30.6 million – a 24% decrease from the 2005 total of £40.3 million. Previously cheque fraud losses had been on the increase, totalling £36 million in 2002 and £45 million in 2003.

Types of cheque fraud

Counterfeit cheque fraud: £2.1 million in 2006 (down 34%)

Cheques manufactured or printed on non-bank paper to look exactly like a genuine cheque and drawn by a fraudster on genuine accounts held by the bank.

Forged cheque fraud: £22.4 million in 2006 (down 28%)

A genuine cheque where part or all of it has been completed by the fraudster. This is the most common type of cheque fraud scam undertaken by organised criminal gangs.

Fraudulently altered cheque fraud: £6.1 million in 2006 (down 2%)

A genuine cheque where part or all of it has been altered by a fraudster.

Common cheque fraud scams

One type of cheque fraud involves the criminal buying goods or services being sold by offering to pay for them with a cheque which has been counterfeited, forged or fraudulently altered. The vendor waits for the cheque to clear before parting with the goods or services being sold, wrongly thinking that the funds cannot be taken from his account at a later date.

Over the past few years organised gangs have started to target consumers selling high-value goods such as cars. Consumers selling a high-value item should be particularly wary of accepting a cheque or banker's draft as it may be stolen or counterfeit.

Another development of this scam involves the fraudster offering a cheque or banker's draft for significantly more than the price of the goods (as ever, anything that sounds too good to be true should set alarm bells ringing but their excuse may sound plausible so just be on your guard).

You are then asked to transfer the amount of the overpayment either to them or to a third party after three days when, it is claimed, the cheque will be cleared.

In these instances the cheque or draft isn't genuine and, whilst banks do all they can to spot and stop such cheques in the clearing system, it may only be after you have received value for the cheque that the genuine cheque owner discovers that money is missing from their account. Consequently, the money paid into your account belongs to them and it may be withdrawn from your account. This can sometimes happen several weeks after the money has been paid into your account because the innocent victim of cheque fraud may not know that a cheque has been stolen from their chequebook for weeks or sometimes months, particularly if they do not check their statement regularly. This means that by the time the money is reclaimed you have probably transferred the 'overpayment' and even handed over the goods you are selling.

What is the banking industry doing to prevent cheque fraud?

From the end of November 2007, the banking industry, through a programme of work led by the Cheque and Credit Clearing Company, is changing the way cheques are processed to benefit customers accepting cheques. It means that for the first time a customer can be sure that after a maximum of six working days (after paying a cheque or banker's draft into their bank account) the money is theirs and they are protected from any loss should the cheque turn out to be fraudulent; the funds cannot be reclaimed without the customer's consent unless the customer is a knowing party to fraud.

Despite this positive change the industry continues to recommend that you should be wary of accepting cheques or bankers' drafts if you don't know or trust the person offering them to you – particularly if they are of high value.

There are also a range of prevention techniques employed at both bank and industry level. At an industry level we are focusing on identifying lost or fraudulent cheques as they pass through the clearing system before there is a victim. The banking industry is also working to raise public awareness of the issue.

This approach is already very successful and in the past year the industry identified more than 90% of all fraudulent cheques as they went through the cheque clearing process.

Another way in which the industry is combating cheque fraud is through the Cheque Printer Accreditation Scheme (CPAS), which was set up in the mid-nineties and is managed by the Cheque and Credit Clearing Company. All printers of cheques are required to be accredited to the scheme and to comply with the regulations for ensuring that cheques are printed to the highest security standards. Security features on cheques are tightly controlled through industry standards, which are particularly effective in combating both counterfeit and fraudulently altered cheques. Banks ensure that customers' chequebooks are only printed by members of CPAS.

Liability for cheque fraud

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

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

From November 2007, however, a customer can be sure that after a maximum of six working days (after paying a cheque or banker's draft into their bank account) the money is theirs and they are protected from any loss should the cheque turn out to be fraudulent – the funds cannot be reclaimed without the customer's consent unless the customer is a knowing party to fraud.

Online fraud

43 Types of online banking fraud
46 Industry measures to prevent online banking fraud

Online banking fraud

In 2006 total losses for online banking fraud from scams such as phishing and Trojans reached £33.5 million; an increase of 44% from 2005.

This fraud is increasing from a very small base, which can often make losses appear to grow rapidly. Last year also saw a huge rise in the volume and sophistication of online fraud attempts, which banks and law enforcement have been largely successful in combating. However a small percentage of attempts do succeed, and it is therefore highly important that customers are aware of the steps they can take to protect themselves. Furthermore, this needs to be seen in context. At £33.5 million, online banking fraud losses are relatively small when compared with total plastic card fraud losses (£428.0 million).

In the second half of the year, enhancements to the fraud prevention systems used by the banks to detect and prevent online banking fraud meant that far more fraud was prevented. This is reflected in the figures, which show that losses were more than halved in the second half of the year compared with the six months from January to June. Online banking fraud losses amounted to £22.5 million in the first half of 2006 but fell to just £11 million between July and December.

Types of online banking fraud

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

Phishing

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

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

There were 14,156 phishing incidents targeted against UK banks and building societies in 2006, up from 1,713 in 2005.

Number of phishing incidents* targeted against UK banks and building societies by month 2005-2006

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513
2005	18	29	27	54	72	122	153	160	190	267	255	353

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

Trojans

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

Money mules

Most of the fraudsters behind these scams are located overseas. As it is not possible to make cross-border transfers out of UK online bank accounts, a money mule or money transfer agent is required to launder the funds obtained as a result of phishing and Trojan scams. After being recruited by the fraudsters, money mules receive funds into their accounts and they then withdraw the money and send it overseas using a wire transfer service, minus a percentage commission payment.
There were 1,087 money mule recruitment incidents in 2006, compared with 473 in 2005.

Number of mule recruitment incidents* by month 2005-2006

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
2006	42	64	96	81	110	75	72	109	109	132	113	84
2005	21	29	28	33	44	41	26	42	40	57	59	53

* Money mule recruitment incidents are measured by the attempts made by a fraudster to recruit individuals to receive funds from compromised accounts. These individuals are then asked to transfer the funds to the fraudsters via money transfer agencies. Mule recruitment incidents are counted by recruitment e-mails or malicious sites.

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

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

Industry measures to prevent online banking fraud

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

A number of initiatives are already in place:

- monitoring of the internet at industry and bank level to detect and close down phishing-related websites;
- two-way communication with online partners so security intelligence can be shared and used effectively; and
- development and use of clear and consistent advice for consumers.

During 2007 one of the initiatives being introduced by some banks to provide a higher level of online banking security is the roll-out of hand-held chip and PIN card reading devices *(see page 32)*. These devices work via a customer inserting their chip and PIN card into a hand-held card reader and entering their PIN. On confirming the PIN entered, the reader generates a unique, one-time only passcode, which the cardholder provides, when prompted, for authentication with their online bank. This solution helps to ensure that the person conducting business online is the genuine customer and will make these types of transaction even safer.

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

Other types of fraud

48 Payment fraud
49 Lending fraud
50 Insider fraud

Payment fraud: £72.2 million in 2006

Payment fraud consists of three fraud categories:

- **Fraudulent encashment** – fraudulent cash or draft withdrawals made over the bank counter.
- **Conversion fraud** – involves collection of a payment by the bank for someone other than the rightful payee. An example is a cheque that is made payable to an organisation but is then paid into a different account from the one it was originally destined for. The introduction of the 'check your cheques' regulation in September 2006 was designed to counter this type of fraud. (Any cheque written to a bank or building society should not be made payable simply to that organisation. Further details have to be added in the payee line, for example XYZ Bank, re: J. Jones, account number 123456).
- **A forged instruction (or forged transfer authority)** – involves a fraudulent payment instruction where the genuine account holder has not issued the instruction. An example is online banking fraud where a fraudster has acquired the login details and passwords of a genuine account (either through a phishing e-mail or Trojan virus) and then accesses and transfers the funds out of the account.

Contained within this category are online banking fraud losses (the majority of which are forged instructions), which totalled £33.5 million in 2006 *(see page 42)*.

What is the industry doing to prevent payment fraud?

There are a number of initiatives in place to tackle this type of fraud such as: sharing best practices; sharing intelligence data between banks; using fraud-detection software to spot and stop this fraud from happening; application of thresholds (where extra checks are made for high value transactions); and continuing review of internal procedures.

Lending fraud:
approximately £160m to £180 million in 2006

To increase transparency across all payment industry fraud types APACS has started work to collate industry-wide fraud figures for lending fraud losses (which includes personal loan, mortgages and unauthorised overdraft losses). This piece of work includes expanding the number of organisations that report figures. APACS is working with its members to collect and develop more robust data during 2007, although early data collected suggests that lending fraud losses in 2006 were in the region of £160m to £180m.

What is lending fraud?

Lending fraud involves money that is lent to someone who is using false information to secure a cash advance such as a mortgage, loan or overdraft – which is subsequently never repaid.

What is the industry doing to prevent lending fraud?

There are a number of initiatives in place to tackle this type of fraud such as: sharing best practices; sharing intelligence data between banks; using fraud-detection software to spot and stop this fraud from happening; application of thresholds (where extra checks are made for high value transactions over a certain value); and continuing review of internal procedures.

Insider fraud

Insider fraud describes a type of compromise rather than a type of fraud – the information that the criminal steals is then used to commit another type of crime, such as card ID theft or fraudulent transactions over the phone or internet. The losses are reported in to APACS under one of these fraud types, rather than as insider fraud – this therefore makes it extremely difficult to quantify exactly what precise losses relate to this type of compromise, although occurrences of insider fraud within the industry are relatively low.

What is insider fraud?

Insider fraud is committed by an employee or an individual employed by a company, who is engaged in criminal activity against their employer or business. Insider fraud can also be committed by contractors or other parties engaged in commercial relationships with a business.

Occurrences of insider fraud are relatively low but, as with all types of fraud, the industry still takes this form of fraud very seriously indeed. Preventing and detecting insider fraud has a high priority with all banks – not least because of the potential negative impact on that organisation's reputation.

What is the industry doing to prevent insider fraud?

Each bank has a myriad of different security checks and controls in place, all of which are kept under constant review. Measures in place include:

- A zero tolerance policy, stipulating that insider fraud will not be tolerated and all such actions will be thoroughly investigated by the bank and passed to the police for prosecution if appropriate.
- Thorough vetting of employees and HR awareness of the issue.
- A mechanism for staff to whistleblow on individuals engaged in insider fraud.
- Staff training about insider fraud – e.g. dos & don'ts, advice on what action to take if there are any concerns, details of the consequences of committing fraud e.g. disciplinary, recovery of monies taken and possible prosecution.
- Audit trails – local and central monitoring of staff activity and transactions.
- APACS has produced a training DVD for its members that helps explain how criminals seek to undertake this type of fraud.
- Control processes and automated management checks.
- Encryption of sensitive data.
- Security policies around the storage and protection of information.
- Use of CCTV.

Contacts & websites

54 Web links
56 Publications
59 Useful contacts

Web links

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

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

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

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

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

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

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

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

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

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

www.dcpcu.org.uk

Explains how the specialist *Dedicated Cheque and Plastic Crime Unit* is tackling the prevention of plastic card and cheque crime.

www.equifax.co.uk

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

www.experian.co.uk

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

www.financial-ombudsman.org.uk

An independent service for resolving disputes between consumers and financial firms.

www.getsafeonline.org

A government and leading business-sponsored site that provides advice on how to protect your computer and safely use the internet.

www.identitytheft.org.uk

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

www.idfraudpreventiontraining.com

Tailored, electronic training courses for businesses to train their employees on how to check the authenticity of documents used to confirm identity.

www.mastercard.com/uk/securecode

Details of how to sign up and benefit from extra protection when shopping online with a MasterCard.

www.paymentscouncil.org.uk

A newly created strategic payments body set up to regulate and represent the payments industry.

www.visaeurope.com/verified

Details of how to sign up and benefit from extra protection when shopping online with a Visa card.

Publications

UK Payment Statistics 2007

A new annual publication that provides a comprehensive source of UK payment statistics and historical data from 1996 to 2006, with additional forecast data up to and including 2016. Available from APACS at a cost of £750.

The Way We Pay – UK Cash and Cash Machines 2007

Examines the main trends in cash payments, the deployment and usage of cash machines, and other forms of cash acquisition. Available from APACS at a cost of £250.

The Way We Pay – UK Plastic Cards 2007

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

The Way We Pay – UK Automated Payments 2007

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

The Way We Pay – UK Cheques 2007

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

Personal Security Plan

A guide for consumers detailing the ways in which fraudsters operate and useful advice on how to avoid being a victim of fraud. Available to download as a PDF from **www.cardwatch.org.uk**.

Spot & Stop Card Fraud retailer training pack

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

Counter Attack

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

Spot & Stop Card-not-Present Fraud

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

Card Force

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

Useful contacts

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

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

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

Mark Bowerman, PR manager
020 7711 6251 M: 07799 627256
mark.bowerman@apacs.org.uk

Rosalind Sellers,
government relations executive
020 7711 6280 M: 07795 146415
rosalind.sellers@apacs.org.uk

British Bankers' Association
020 7216 8800

DCPCU
Media enquiries: 020 7711 6340

Call Credit
0870 060 1414

CIFAS
0870 010 2091

Experian
0870 241 6212

Financial Ombudsman Service
0845 080 1800

Royal Mail Customer Enquiries
08457 740740

Bank and building society contacts

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

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

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

Bank of Scotland (HBOS)
Switchboard: 0870 600 5000
Press office: 0131 243 7077
pressoffice@hbosplc.com

Barclays Bank
Switchboard: 020 7116 1000
Press office: 020 7116 4755
elizabeth.holloway@barclays.co.uk
www.barclays.co.uk

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

Capital One
Switchboard: 0115 843 3300
Press office: 0115 843 3676
sally.camm@capitalone.com
www.capitalone.co.uk

Citigroup
Switchboard: 020 7986 4000
Press office: 020 7986 5602
adrian.russell@citigroup.com
www.citigroup.com

Clydesdale Bank
Switchboard: 0141 248 7070
Press office: 0141 242 4165
stuart.neill@eu.nabgroup.com
www.cbonline.co.uk

Co-operative Bank
Switchboard: 0161 832 3456
Press office: 0161 829 5397
andy.hammerton@co-op.co.uk
www.co-operativebank.co.uk

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

Egg
Switchboard: 020 7220 25088
Press office: 020 7150 2657
pressoffice@prudential.co.uk
www.egg.com

GE Capital
Press office: 020 7853 1831
robert.buller@ge.com
www.gemoney.co.uk/en/

Halifax (HBOS)
Switchboard: 0870 600 5000
Press office: 01422 333 829
pressoffice@halifax.co.uk
www.hbosplc.com

HFC Bank
Switchboard: 01344 890 000
Press office: 01344 892411
patrick.long@hfcbank.co.uk
www.hfcbank.co.uk

HSBC/First Direct
Switchboard: 020 7991 8888
Press office: 020 7991 1573/3756
pressoffice@hsbc.com
www.hsbc.com

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

MBNA Europe Bank
Switchboard: 01244 672 000
Press office: 01244 574136
paul.lawler@mbna.com
www.mbna.com

Morgan Stanley
Switchboard: 020 7425 8000
Press office: 020 7269 7171
denise.macfarlane@morganstanley.com
www.goldfish.com
www.morganstanley.com/card

National Australia Bank
Switchboard: 020 7710 2100
Press office: 0113 247 2510
peter.brown@eu.nabgroup.com
www.national.com.au

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

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

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

The Royal Bank of Scotland
Switchboard: 0131 556 8555
Retail bank press office: 020 7672 1922
laura.mottram@rbs.co.uk
www.rbs.co.uk

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

Card scheme contacts

VISA International
Switchboard: 020 7937 8111
Press office: 020 7795 5463
europeanmedia@visa.com
www.visa.com

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

American Express
Switchboard: 01273 693 555
Press office: 020 7976 4418
doug.w.smith@aexp.com
www.americanexpress.com

Diners Club
Switchboard: 0870 190 0011
Press enquiries: 0870 190 0011
www.dinersclub.com

APACS is the trade body that gives banks, building societies and card issuers a forum where they can work together on non-competitive issues. In a nutshell we help manage the way that businesses and individuals in the UK move their money around – this covers cash, credit and debit cards, cheques and automated payments such as direct debits, salary payments and online/phone transactions.
We also champion the fight against banking fraud and are the people who have been working to give consumers greater card fraud protection by introducing chip and PIN. Twice a year we publish figures on banking fraud losses.

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

APACS
the UK payments association

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