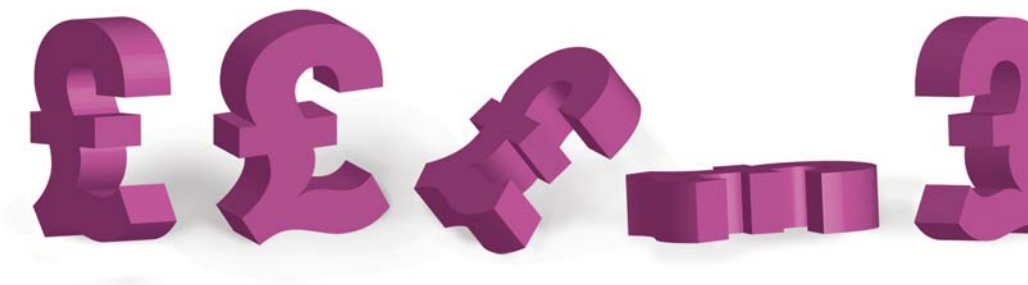
Fraud
The Facts 2008



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

APACS

APACS, the UK payments association, is the trade body that gives banks, building societies and card issuers a forum where they can work together on non-competitive issues. 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 lead the fight against banking fraud and twice a year we publish figures on payment industry fraud losses.

"Although card fraud levels have now begun to increase again due to fraud abroad and card-not-present fraud losses, chip and PIN has proven to be an undoubted success in reducing card fraud on the UK high street.

"The banking industry continues to work with law enforcement, the retail sector, the Home Office and organisations such as the charity Crimestoppers. This reflects the multi-layered approach needed to provide both short-term and long-term solutions to protect customers against all types of banking fraud."

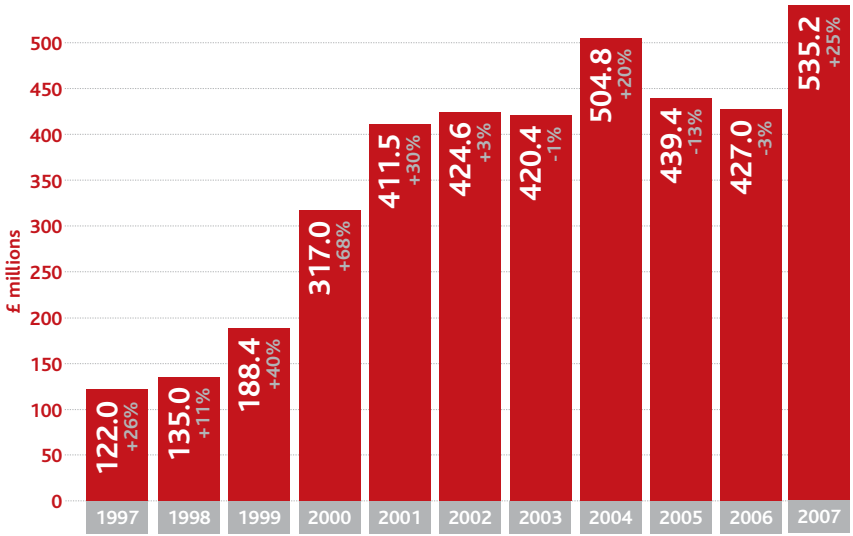
Katy Worobec, APACS Head of Fraud Control

Contents

Plastic card fraud

Plastic card fraud losses on UK-issued cards 1997-2007

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



Annual plastic card fraud losses on UK-issued cards 1997-2007

All figures in £ millions

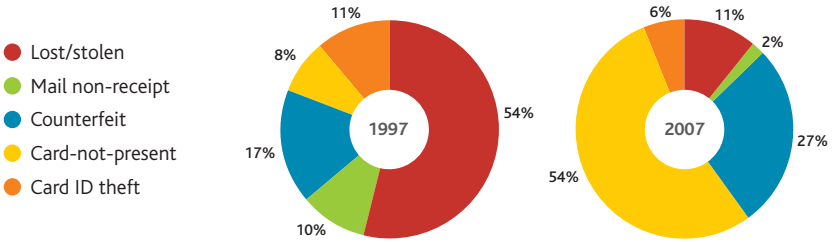
Fraud type	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Card-not-present	10.0	13.6	29.3	72.9	95.7	110.1	122.1	150.8	183.2	212.7	290.5
Counterfeit	20.3	26.8	50.3	107.1	160.4	148.5	110.6	129.7	96.8	98.6	144.3
Lost/stolen	66.2	65.8	79.7	101.9	114.0	108.3	112.4	114.5	89.0	68.5	56.2
Card ID theft	13.1	16.8	14.4	17.4	14.6	20.6	30.2	36.9	30.5	31.9	34.1
Mail non-receipt	12.5	12.0	14.6	17.7	26.8	37.1	45.1	72.9	40.0	15.4	10.2
Total	122.0	135.0	188.4	317.0	411.5	424.6	420.4	504.8	439.4	427.0	535.2
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	73.0
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	309.9	327.6
Fraud abroad	29.2	34.9	54.2	103.5	138.4	130.2	104.1	92.5	82.8	117.1	207.6

* Due to the rounding of figures, the sum of separate items may differ from the totals shown.

Overview

Whilst card usage and transaction volumes continue to grow, plastic card fraud losses against total turnover – at 0.118% – are still significantly less than in 2001 (before the introduction of chip and PIN), when fraud-to-turnover was 0.183%.

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



* *(See table opposite)* The most marked regional increases in fraud – in the East and West Midlands – are down to larger than average increases in card-not-present fraud losses. However, because of the nature of this crime it does not necessarily mean that these regions are hotspots for this particular type of fraud. A number of card-not-present retail head offices are located in these particular regions – the figures may be reported into us according to the head office location rather than the precise location of the fraud.

Plastic card fraud losses in the UK on UK-issued cards split by UK region 2004-2007

All figures in £ millions

Region	2004	2005	2006	2007	+/- change 06/07
South East	£238.2	£207.3	£176.6	£178.7	+1%
North West	£40.2	£33.2	£35.7	£35.8	0%
West Midlands*	£24.2	£20.3	£17.2	£24.4	+42%
Yorkshire & Humberside	£24.3	£27.3	£27.2	£24.1	-11%
East Midlands*	£30.8	£23.8	£15.0	£22.8	+52%
South West	£12.7	£11.3	£9.7	£11.8	+22%
Scotland	£16.7	£13.9	£9.9	£11.5	+16%
North East	£8.1	£7.3	£6.8	£7.8	+15%
Wales	£7.3	£5.2	£5.7	£5.3	-7%
East Anglia	£8.7	£6.2	£5.4	£4.8	-11%
Northern Ireland	£1.1	£0.8	£0.7	£0.7	0%
UK total	£412.3	£356.6	£309.9	£327.6	+6%
Fraud abroad	£92.5	£82.8	£117.1	£207.6	+77%
Total all UK cards	£504.8	£439.4	£427.0	£535.2	+25%

Phone, internet and mail order (card-not-present or CNP) fraud: £290.5 million in 2007 (up 37%)

This crime most commonly involves the theft of genuine card details in the real world that are then used to make a purchase over the internet, by phone, or by mail order. The genuine cardholder may not be aware of this fraud until they check their statement.

It is the largest type of card fraud in the UK.

However, these losses should be seen in the context of huge increases in both the amount of people shopping online and over the phone, and the number of retailers offering telephone or online shopping. Since the year 2000, phone, internet and mail order fraud losses have risen by 298 per cent. Over the same time period, the total value of online shopping transactions alone increased by 871 per cent (up from £3.5 billion in 2000 to £34 billion in 2007). More than 30 million UK adults shop online.

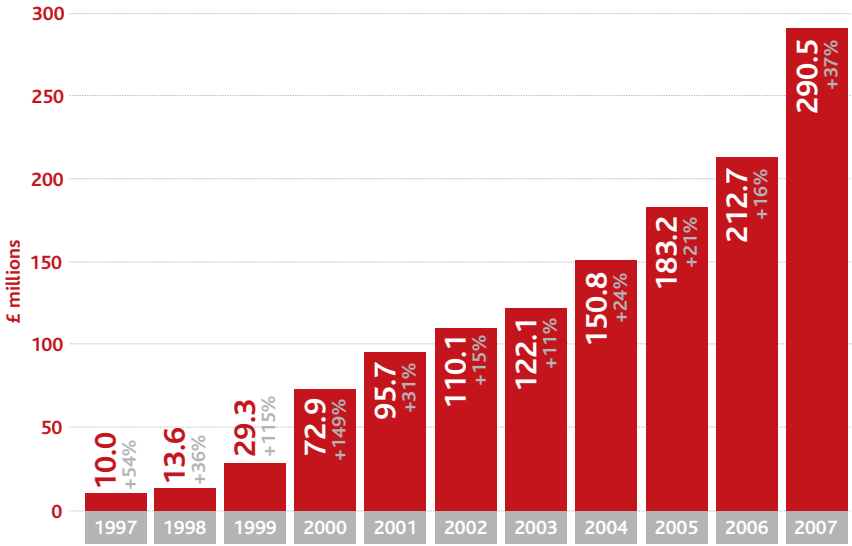
The difficulty in countering this type of fraud lies in the fact that neither the card nor the cardholder is present when the transaction happens. This means that:

- Businesses accepting these transactions are unable to check the card's physical security features to determine whether it is genuine.
- Without a signature or a PIN there is less certainty that the customer is the genuine cardholder.

A number of initiatives are available to help businesses protect themselves from this type of fraud, such as address verification and card security code software, and MasterCard SecureCode and Verified by Visa. See page 31 for more details.

Card-not-present fraud losses on UK-issued cards 1997-2007

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



Counterfeit card fraud: £144.3 million in 2007 (up 46%)

Counterfeit card fraud occurs when a fake card is created using compromised card details, often stolen by fraudsters from the magnetic stripe of a genuine card.

Counterfeit card fraud losses in the UK continue to decrease (down 71% between 2004 and 2007), because chip and PIN has made it much harder for criminals to use fake cards in cash machines and shops in the UK.

This type of fraud is increasing overall because criminals continue to carry out old-style card fraud by targeting the magnetic stripe on the back of UK chip and PIN cards. Fraudsters copy the magnetic stripe details, typically by skimming cards, then create fake magnetic stripe cards that they use overseas in countries that do not have 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% year-on-year, whereas the equivalent losses overseas have increased by 114%.

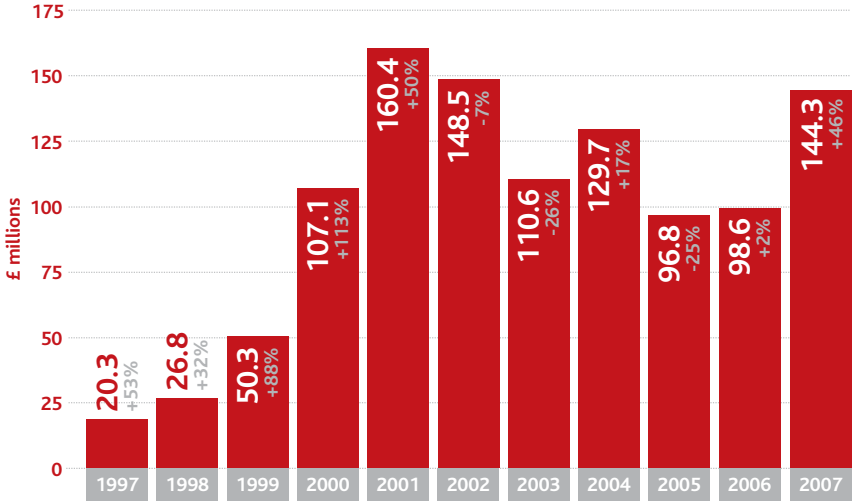
Counterfeit card fraud losses in the UK and abroad 2004-2007

All figures in £ millions

Region	2004	2005	2006	2007	+/- change 06/07
Domestic (in the UK)	£105.9	£78.6	£45.8	£31.1	-32%
Abroad	£23.8	£18.2	£52.8	£113.2	+114%
Total	£129.7	£96.8	£98.6	£144.3	+46%

Counterfeit card fraud losses on UK-issued cards 1997-2007

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



Lost and stolen card fraud: £56.2 million in 2007 (down 18%)

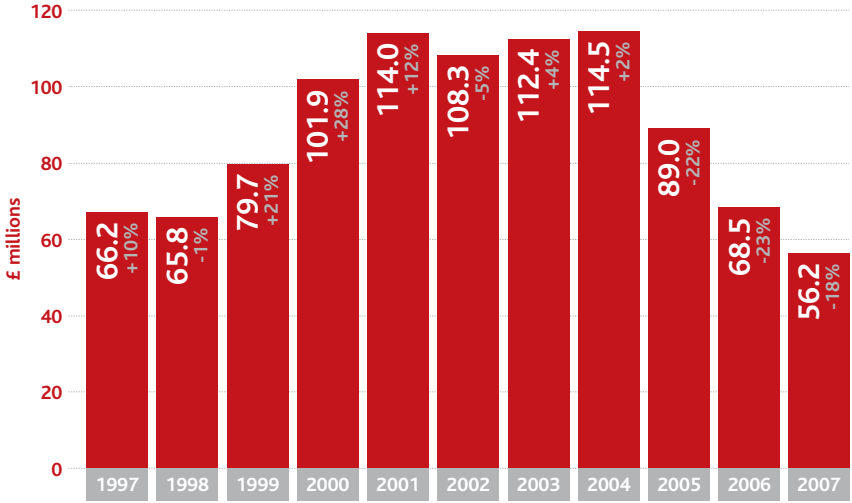
This category covers fraud on cards that have been reported by the cardholder as lost or stolen. Lost and stolen cards could be used in shops that do not have chip and PIN equipment, or they could potentially be used to commit fraud via a phone, internet or mail order transaction.

Thanks to the introduction of chip and PIN this type of card fraud is now at its lowest level for ten 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 enables retailers to check electronically whether a card has been reported lost or stolen;
- A retailer education programme, run by APACS since 2001, 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**.

Lost and stolen fraud losses on UK-issued cards 1997-2007

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



Mail non-receipt fraud: £10.2 million in 2007 (down 34%)

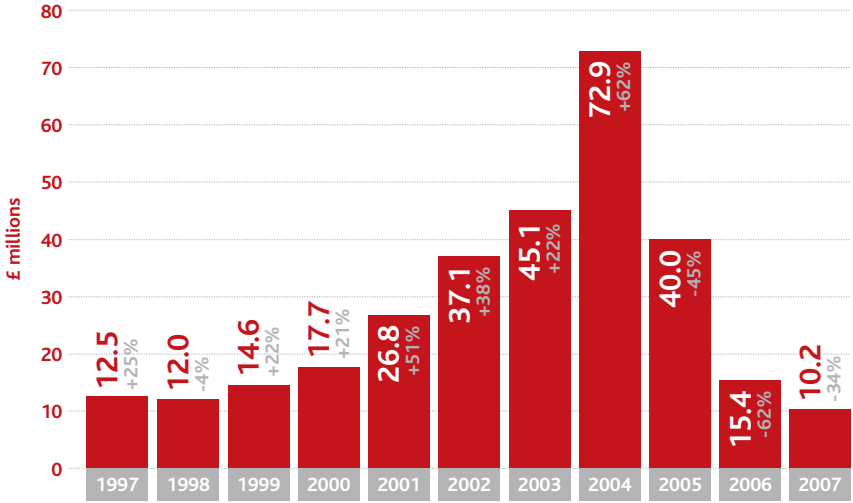
This type of fraud involves cards being stolen in transit – after card companies send them out and before the genuine cardholders receive them. Particularly at risk for this type of fraud are properties with communal letterboxes, such as flats and student halls of residence and people who do not get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

This type of fraud decreased by 34% to £10.2 million in 2007, and now represents less than 2% of total card fraud losses. In fact, mail non-receipt fraud is now at its lowest level for ten years. The main reason behind this large decrease is because there are fewer cards and PINs being sent out than in the past few years, when chip and PIN cards were being issued to UK cardholders. This means there are fewer opportunities for cards to be intercepted. Also, when replacement cards are issued, the cardholder already knows the PIN, so the PIN is not sent out. So, if a fraudster intercepts the card, he is unlikely to be able to use the card at a shop or cash machine in the UK.

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.

Mail non-receipt fraud losses on UK-issued cards 1997-2007

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



Card ID theft: £34.1 million in 2007 (up 7%)

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 held in someone else's name.

Collectively, card ID theft rose by 7% in the past year to £34.1 million, and now accounts for just over 6% of overall card fraud losses.

This type of fraud can be split into two categories: third-party application fraud and account takeover fraud.

Application fraud: £11.7 million in 2007 (down 2%)

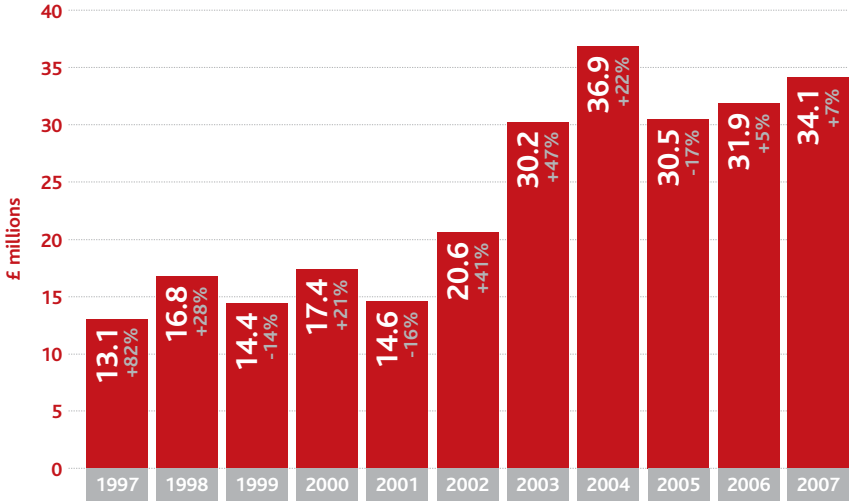
Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeited documents for identification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

Account takeover: £22.4 million in 2007 (up 12%)

This involves a criminal fraudulently using another person's credit or debit card 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 1997-2007

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 particularly countries overseas that have not yet upgraded to chip and PIN.

UK retailer (face-to-face) fraud: £73.0m in 2007 (up 1%)

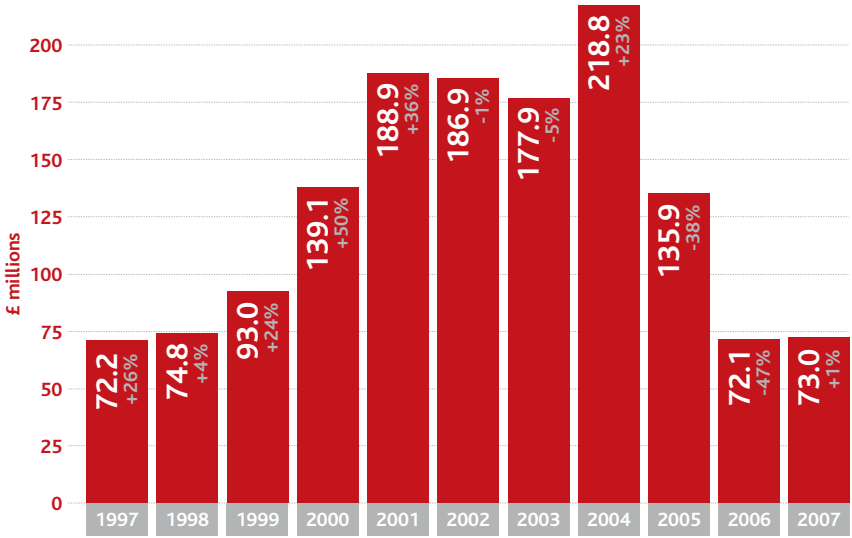
Chip and PIN has meant that card fraud losses in the UK high street have declined by 67% since peaking at £218.8 million in 2004. There was a 1% increase in 2007.

One of the ways in which this fraud happens is through criminals using lost and stolen cards. These can potentially be used at shops in the UK, especially if a cardholder has written the PIN down, for example, and stored it in their purse or wallet and had that stolen too.

A smaller proportion of this fraud will consist of transactions on cards being used fraudulently as a result of card ID theft or mail non-receipt fraud.

Card fraud losses at UK retailers (face-to-face transactions) 1997-2007

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



Cash machine fraud: £35.0 million in 2007 (down 44%)

These fraud losses show the amount of money withdrawn fraudulently at UK cash machines, on UK-issued cards. Dropping by 44% last year alone, to £35.0 million, these losses now account for less than 7% of total card fraud.

Despite the number of UK cash machines almost tripling in the last ten years to more than 60,000, cash machine fraud has fallen dramatically in the past three years because of chip and PIN. The introduction of chip and PIN has meant that fraudsters are now being forced to use fake magnetic stripe cards in cash machines overseas, in countries that haven't yet upgraded. A large proportion of the cash machine fraud total is still the result of cardholders writing down their PIN and keeping it with their purse or wallet, which is then stolen.

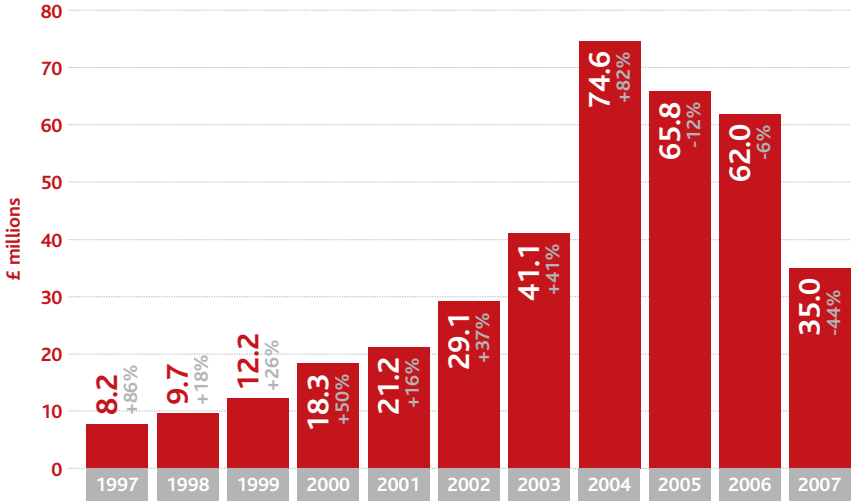
Cash machines can also be a target for fraudsters as a point of card compromise, where they attempt to steal cards or card details.

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

- 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. A miniature camera is also 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 yet upgraded to chip and PIN.

Fraud losses at UK cash machines 1997-2007

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



- Shoulder surfing – criminals observe the PIN being entered by the cardholder, then steal the card using distraction techniques or pickpocketing, before using the stolen card and genuine PIN.

Fraud abroad: £207.6 million in 2007 (up 77%)

The successful introduction of chip and PIN in the UK means that fraudsters are increasingly being driven overseas to commit card fraud in those countries that have not yet rolled out chip and PIN.

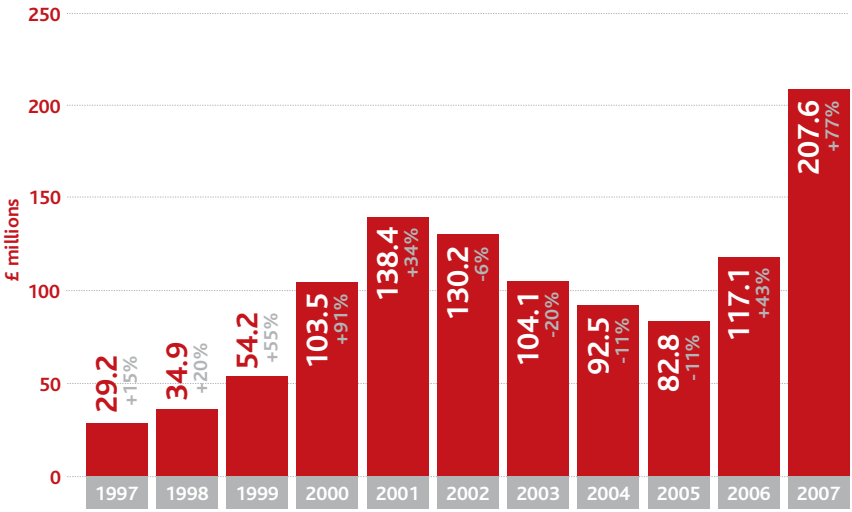
Criminals are stealing magnetic stripe card details from our cards in the UK and then making fake magnetic stripe cards that are used overseas in countries yet to upgrade to chip and PIN. At £207.6 million, fraud abroad now accounts for more than one third (39 per cent) of total card fraud losses.

The countries where fraud abroad is occurring on UK-issued cards have changed over the past three years; there has been a marked decline in France and Spain as those countries continue their chip and PIN rollout. Fraud on UK-issued cards in the USA, however, has increased by 118% since 2005, to £24.6 million in 2007. It is now the top country for fraud abroad committed on UK-issued cards. Italy and Australia have also moved into the top three, with fraud at £9.6 million and £8.2 million respectively.

As more and more countries around the world progress their chip and PIN rollouts, it is expected that fraud will continue to shift towards countries such as the US, which as yet has no plans to implement chip and PIN.

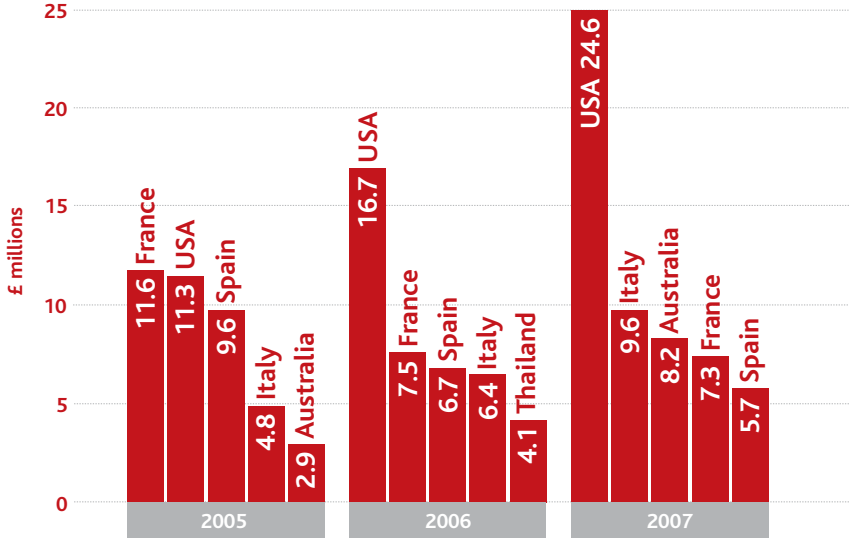
Fraud committed abroad on UK-issued cards 1997-2007

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



Top 5 countries for fraud abroad 2005-2007

(UK-issued cards or card details used fraudulently overseas)



Internet/e-commerce fraud on cards:
estimated at £223.8 million in 2007 (up 45%)

£223.8m of card fraud took place over the internet in 2007 – 77% of total card-not-present fraud losses. This figure has gone up by 45% from 2006, when e-commerce fraud losses were £154.5m and accounted for 73% of card-not-present 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, data hacking or through unsolicited emails or telephone calls. The card details are then used to make fraudulent card-not-present transactions, most commonly via the internet. As the number of internet retailers has grown, fraudsters have increasingly targeted the online shopping environment.

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. It has proven to be an undoubted success in reducing particular areas of card fraud:

- Over the past three years, losses on face-to-face transactions on the UK high street have reduced by 67% from £218.8m in 2004 to £73.0m last year.
- Fraud on lost and stolen cards (£56.2m) and mail non-receipt fraud (£10.2m) are now at their lowest levels for 10 years.
- UK cash machine fraud has decreased by 44%, last year.
- Domestic levels of counterfeit card fraud have decreased by 32% in the past year.

The UK has been the international leader in implementing the global standard for chip and PIN. APACS and its members were instrumental in the development of this standard, and the UK was the first country in the world to complete the rollout of this global chip and PIN system. As more and more countries roll out chip and PIN, our cards will become safer – not just in the UK, but all over the world.

Dedicated Cheque and Plastic Crime Unit (DCPCU)

A specialist police unit targeting organised criminal gangs

The Dedicated Cheque and Plastic Crime Unit (DCPCU) is a special police unit fully sponsored by the banking industry, through APACS, and has an ongoing brief to help stamp out organised card and cheque fraud across the UK. It is a unique body that comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators.

The unit was responsible for £107 million in estimated fraud savings in 2007. This compares with savings of £130 million achieved in the five years following the unit's launch in 2002. This huge boost in annual performance reflects a significant increase in the number of counterfeit cards and card details recovered by the unit. Their work last year disrupted 421 organised crime networks, leading to the recovery of:

- 103,000 compromised card details
- 16,500 counterfeit cards
- 7,000 fraudulent cheques

The unit is comprised of three operational teams, which are supported by a newly-created intelligence arm, the Payments Industry and Police Joint Intelligence Unit.

Payments Industry & Police Joint Intelligence Unit (PIPJIU)

A joined-up approach to tackle fraud

Launched in March 2008, the PIPJIU forms an integral part of the Dedicated Cheque and Plastic Crime Unit (DCPCU). It is an enhanced intelligence unit formed through the amalgamation of the banking industry's Fraud Intelligence Bureau (FIB) – the body that formerly distributed information between the banking industry and law enforcement throughout the UK – and the intelligence section of the DCPCU.

As well as providing a more efficient approach to the collation and dissemination of fraud intelligence to police forces throughout the country, this new unit has wider-reaching responsibilities to address all types of banking fraud – not just cheque and plastic card fraud.

The PIPJIU is staffed by banking industry fraud specialists who work alongside officers from the City of London and Metropolitan Police.

Fraud Intelligence Sharing System

Sharing intelligence to tackle fraud

In addition to the creation of the PIPJIU, APACS has also established a new Fraud Intelligence Sharing System (FISS) which, through the PIPJIU, will enable the banking industry to share information on all confirmed, attempted and suspected fraud in a central, shared database. Established specifically to combat banking-related fraud in the UK, the system provides the industry with a secure and robust reporting mechanism, supporting the industry's long-term fraud prevention strategy.

Industry Hot Card File (IHCF)

Checking every card transaction for cards being used fraudulently

The IHCF contains information on more than 6 million cards that have been reported lost or stolen. During the last two years, over 700,000 cases of attempted fraud have been prevented by this system. The IHCF is also being used successfully at motorway tollbooths in France to combat the use of stolen UK cards at road tolls.

More than 80,000 retailers subscribe to this electronic file. 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 any of those on the system.

The IHCF is increasingly being used by retailers that operate in the card-not-present environment, and has provided a mechanism for checking card details prior to the goods being dispatched. Extending its use into other environments for fraud prevention purposes are under consideration.

CIFAS – the UK's Fraud Prevention Service

Sharing information to stop fraud

CIFAS is a fraud prevention body that provides services to its members, spread across banking, credit cards, mail order, insurance, telecommunications and other sectors. It enables them 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.

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 67% from £218.8 million in 2004, to £73.0 million last year. Face-to-face card fraud now represents just 14% of total card fraud losses (down from 59% in 1996), despite the number of cards in issue increasing by 72% over the past ten years, and the number of shop terminals doubling over the same time period.

A very small percentage of businesses have yet to upgrade to chip and PIN, and APACS continues to work with these retailers, using its Spot & Stop Card Fraud education pack. 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 education pack is available at **www.cardwatch.org.uk**.

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

Helping businesses fight CNP fraud

Although phone, internet and mail order 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. Cardholders are prompted to register with Verified by Visa and MasterCard SecureCode whenever they shop online at a participating retailer's website. 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 retailer when a genuine customer is using their card online. More than 20 million cards have already been registered for these systems. To find out more, please visit **www.visaeurope.com/personal** and **www.mastercard.com/uk/personal/en.**
- An automated cardholder address verification and card security code (AVS/CSC) system is available for businesses that accept phone, internet and mail order 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 third party providers is available at **www.cardwatch.org.uk.**
- APACS' Spot & Stop Card-not-Present Fraud pack provides comprehensive fraud prevention training for businesses that accept phone, internet or mail order payments. An e-learning version is available at **www.cardwatch.org.uk.**

Using chip and PIN to help prevent remote channel fraud

Hand-held card readers that create one-time passcodes

One potential 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 (e.g. phone and internet shopping). One solution – hand-held card readers – builds upon chip and PIN technology and, for remote shopping, could enhance the online protection already offered by systems such as MasterCard SecureCode and Verified by Visa.

It works by 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 began to see the rollout of these devices in the latter part of 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 whether 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 6% – prevention measures remain in place (and will continue to be developed) to combat this type of fraud.

The banking industry sits on a Home Office Identity Fraud Steering Committee, which consists of senior representatives from the public and private sectors, and brings together all those with an interest in reducing identity fraud in the UK.

A sub-group of this committee, the Identity Fraud Communications Awareness Group (IFCAG) which includes representatives from APACS, the British Bankers' Association and CIFAS, has created a bespoke website for ID fraud prevention at **www.identitytheft.org.uk.**

The site also advises the public how best to protect themselves from identity theft and offers advice for victims. This is complemented with a range of leaflets and posters for use in public areas including libraries, Citizens Advice Bureaux and bank counters. It will soon provide best practice guidelines for businesses that could be targeted by identity fraudsters, and 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.

Industry measures to prevent cash machine crime

Multi-layered approach to tackling fraud

Although UK cash machine fraud losses have decreased by 53% over the past three 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 crime.

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

- 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 near.
- 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.
- Use of CCTV to deter criminal activity.

Cheque fraud

What is cheque fraud?

There are three types of cheque fraud in the UK: counterfeit, forged, and fraudulently altered cheques.

Following significant year-on-year reductions in 2005 and 2006, cheque fraud losses in 2007 rose 10% to £33.5 million. However, they still remain relatively low compared with other fraud types.

Types of cheque fraud

Counterfeit cheque fraud: £3.8 million in 2007 (up 81%)

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

Forged cheque fraud: £20.5 million in 2007 (down 9%)

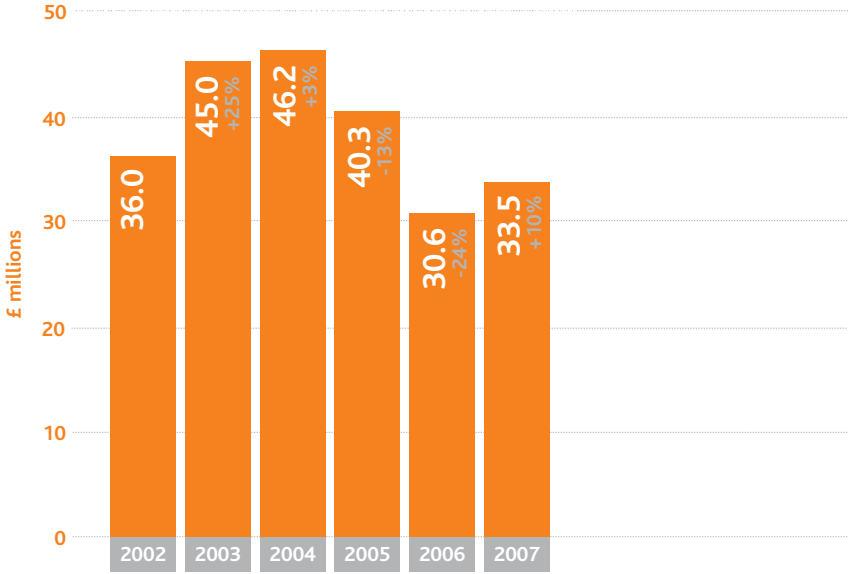
A forged cheque is a genuine cheque that has been stolen from an innocent customer and used by the fraudster with a forged signature.

Fraudulently altered cheques: £9.2 million in 2006 (up 51%)

A fraudulently altered cheque is a genuine cheque that has been made out by the payer, but a fraudster has altered the cheque in some way before it was paid in, e.g. by altering the beneficiary's name or the amount of the cheque.

Cheque fraud losses 2002-2007

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



Common cheque scams

There are a number of ways in which scams involving cheques can be carried out. They may involve not only stolen or fraudulent cheques and bankers' drafts, but also genuine cheques owned by the fraudster, which subsequently bounce due to lack of sufficient funds. The following examples illustrate two common cheque scams.

Over recent years organised gangs have targeted consumers selling high-value goods such as cars. When selling a high-value item, customers should be particularly wary of accepting a cheque or banker's draft – criminals use stolen or counterfeit cheques and bankers' drafts. Anyone who does accept a cheque is advised not to hand over the goods until they have certainty that the cheque funds will not be reclaimed (this happens at the end of the sixth day after they have paid the cheque into their account).

One 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 the fraudster's excuse may sound plausible so be on guard.

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

It is likely that the cheque or draft is fraudulent, and the banks do all they can to spot and stop such cheques and drafts in the clearing system. However, with this scam, the cheque might be genuine, but the fraudster does not have sufficient funds in their account. The paying bank will therefore return the cheque unpaid. If the customer has already made the overpayment to a third party, they will lose the funds – with the 2-4-6 clearing timescales, it is not until the end of the sixth working day after the cheque has been paid in that the customer can be sure that the funds are theirs, and will not bounce.

What is the banking industry doing to prevent cheque fraud?

In November 2007, the banking industry introduced changes known as 2-4-6 to cheque clearing timescales to protect customers accepting cheques from fraud. It means that for the first time a customer can be sure that at the end of six working days (after paying in a cheque) 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 customers should be wary of accepting cheques or bankers' drafts if they don't know or trust the person offering them – particularly if they are of high value.

There is also a range of prevention techniques employed at both bank and industry level. At an industry level, banks continue to focus on identifying lost, stolen 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 stopped more than 90% of all attempted cheque frauds 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 cheque fraud. Banks require that customers' chequebooks are printed only by members of CPAS.

Liability for cheque fraud

Any innocent customer whose chequebook is used by a fraudster will continue to enjoy full protection from any financial loss, provided they haven't breached their terms and conditions.

Following the introduction of the 2-4-6 cheque changes, a customer can be sure that at the end 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. However, any customers who do not wait until the end of day six, and decide to withdraw and spend funds before that, do so at their own risk. If the cheque subsequently bounces, they may have to return funds to their bank or building society.

Online banking fraud

Online banking fraud

In 2007, total losses for online banking fraud from scams such as phishing and spyware were £22.6 million – a decrease of 33% from the previous year (£33.5 million in 2006).

Although attempts by fraudsters increased during 2007, losses declined for a variety of reasons. Efforts to educate customers about the threat of phishing and spyware are paying off, and customers have become more security aware. Banks have also been increasingly successful at detecting and preventing suspicious transactions. Another factor for some banks has been the introduction of stronger methods of authenticating customers, such as the 'chip and PIN at home' devices introduced last year.

Types of online banking fraud

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

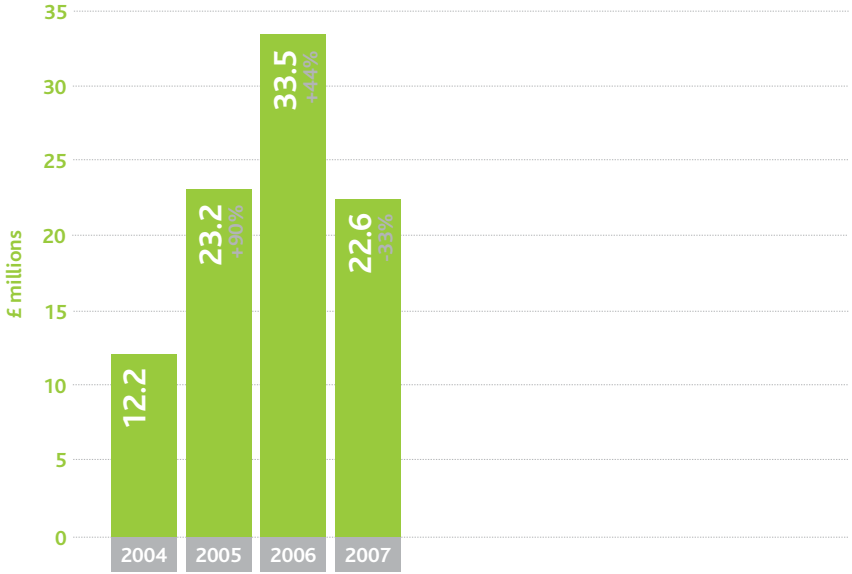
Phishing

Phishing is the name given to the practice of sending emails 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 emails usually claim that it is necessary to 'update' or 'verify' your password, and they urge you to click on a link from the email 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, targeting individual internet users in order to gain personal or secret information that can be used online for fraudulent purposes.

Online banking fraud losses 2004-2007

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



There were 25,797 phishing websites targeted against UK banks and building societies in 2007, up from 14,156 in 2006, which was in turn an increase on 1,713 in 2005.

Number of phishing websites* targeted against UK banks and building societies by month 2005-2007

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195
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

* 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 emails trying to convince people to click on a link that will send them to that fake site.

Spyware

Spyware is a type of computer virus that can be installed on your computer without you realising. Spyware is sometimes capable of acting as a 'keystroke logger', capturing all of the keystrokes entered into a computer keyboard. Typically the fraudsters will send out emails at random, to get people to click on a link from the email and visit a malicious website, where vulnerabilities on the customer's computer are exploited to install the spyware. The emails are not normally related to internet banking, and try to dupe people into visiting, or clicking on the link to, the malicious website using a variety of excuses.

Money mules

Most of the fraudsters behind these scams are located overseas, and they need an accomplice with a UK bank account to act as a "money mule" or money transfer agent, to launder the funds obtained as a result of phishing and spyware scams. Some mules are recruited under false pretences, in the belief that they are being recruited to work for a legitimate company. 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 1,462 money mule recruitment incidents in 2007, compared with 1,087 in 2006.

Money mules are recruited by a variety of methods, including spam emails, adverts on genuine recruitment websites, approaches to people with their CVs displayed 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 money mules may become embroiled in a police investigation. Money mules will be the easiest part of the chain to track down.

Number of mule recruitment adverts* by month 2005-2007

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
2007	77	128	144	99	91	116	123	142	148	110	163	121
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

* These are calculated according to each time a new fake "job" advert is detected. Such scams may appear as spam emails, spoof websites, adverts on real job recruitment websites or even in national newspapers.

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
- Development and use of clear and consistent advice for consumers

During 2007, one of the initiatives introduced by some banks to provide a higher level of online banking security was the rollout of hand-held chip and PIN card reading devices. 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 customers stay safe while banking online. Sections on the site include: types of online banking scams; how to spot them; and how to protect yourself from falling victim. 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.

Facts and figures 2007

Plastic cards

- There were 144.7 million payment cards in issue in the UK at the end of 2007, which included:
  - 71.6 million debit cards
  - 73 million credit and charge cards
- Over 9.9 billion transactions were made on UK cards in 2007, to a total value of £567.7 billion.
- The average number of cards per person in 2007 was 3.6.
- Spending on plastic cards in the UK amounted to £354 billion last year, which comprised £221 billion on debit cards, and £133 billion on credit and charge cards.
- Internet card spending has risen nearly four-fold over the last five years to £34 billion in 2007.

Cash machines

- There were 63,420 cash machines in the UK at the end of 2007.
- There were 2.8 billion cash withdrawals from cash machines in the UK last year – an average of 90 per second.
- The total value withdrawn from cash machines in the UK was £186 billion in 2007 – an average of £5,903 per second.
- The average cash withdrawal at a bank or building society-owned cash machine last year was £67 and £52 at an independently-owned machine.

Cheques

- There were just over 4.4 million business and personal cheques issued each day in 2007, compared with 11 million in the peak year for cheque volumes, 1990.
- Adults receive fewer than five cheques on average per year.
- The average value of a personal cheque payment in 2007 was £230.
- Only 5 million adults still use guaranteed cheques on a regular basis, compared with 15 million in 1996.
- Only 4% of retail spending is still paid by cheque, compared with over 60% by debit or credit card.

Online banking

- Over 20 million adults banked online in 2007.
- 55% of internet users bank online.
- Use is highest among 24 to 35 year olds, where over two thirds of internet users access at least one account online.
- 93% of online bankers access their main current account.

Contacts & websites

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.cifas.org.uk
The UK's fraud prevention service, CIFAS 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 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 use the internet safely.

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.paymentscouncil.org.uk

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

www.shopsafeonline.org.uk

Information for businesses and cardholders about Mastercard SecureCode and Verified by Visa, what they are and how they work.

Publications

UK Payment Statistics 2008

A new annual publication that provides a comprehensive source of UK payment statistics and historical data from 1997 to 2007, 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 2008

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 2008

Details 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 2008

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 2008

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

The Way We Pay – UK Consumer Payments 2008

Looks in detail at consumer holdings and use of different payment methods. Available from APACS at a cost of £1,500.

For more information or to order any of these publications please contact **corpcomms@apacs.org.uk**

Fraud prevention materials

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.

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.

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.

To order these and other fraud prevention materials please visit **www.cardwatch.org.uk.** Interactive training is also available on the site.

Useful contacts

APACS
020 7711 6259
press@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, Public affairs manager
020 7711 6280 M: 07795 146415
rosalind.sellers@apacs.org.uk

Banking Code Standards Board
0845 230 9694

British Bankers' Association
020 7216 8800

Building Societies Association
020 7520 5900

CIFAS - the UK's Fraud Prevention Service
0870 010 2091

Credit Reference Agencies
Call Credit 0870 060 1414
Equifax 0870 010 0583
Experian 0870 241 6212

DCPCU
020 7711 6340 (media enquiries)

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 5952
mediarelations@abbey.com
www.aboutabbey.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 America
Switchboard: 020 7174 4000
Press office: 020 7174 5401
christiana.marran@bankofamerica.com
www.bankofamerica.com

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

Bank of Ireland
Switchboard: 0845 309 8099
Press office: 020 7634 3477
sandra.grandison@boiuk.com
www.bank-of-ireland.co.uk

Bank of Scotland (HBOS)
Switchboard: 0870 600 5000
Press office: 0131 243 7077
pressoffice@hbosplc.com
www.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 3676/6484
sally.camm@capitalone.com
becky.paterson@capitalone.com
www.capitalone.co.uk

Citibank
Switchboard: 0800 00 88 00
Press office: 020 7508 7355
adrian.russell@citi.com
www.citibank.co.uk

Clydesdale & Yorkshire Bank
Switchboard: 0141 248 7070
Press office: 0845 603 5447
press.office@nab.co.uk
www.cbonline.co.uk
www.ybonline.co.uk

Co-operative Bank
Switchboard: 0161 832 3456
Press office: 0161 827 5617
duncan.bowker@co-op.co.uk
www.co-operativebank.co.uk

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

Egg
Switchboard: 01338 395 919
Press office: 020 7508 7355
prteam@egg.com
www.egg.com

GE Capital
Switchboard: 0870 126 2665
Press office: 020 7853 1831
robert.buller@ge.com
www.gemoney.co.uk/en/

Goldfish
Switchboard: 01236 797 800
Press office: 01236 797 425/568
graeme.keddie@goldfish.com
jenny.sutherland@goldfish.com
www.goldfish.com

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
kirsty.clay@lloydstsb.co.uk
www.lloydstsb.com

MBNA Europe Bank
Switchboard: 01244 672 000
Press office: 01244 574136/404
paul.lawler@mbna.com
john.greaves@mbna.com
www.mbna.com

Morgan Stanley
Switchboard: 020 7425 8000
Press office: 020 7425 8005
mediainquiries@morganstanley.com
www.morganstanleycard.co.uk

Nationwide
Switchboard: 01793 656 789
Press office: 01793 655 198
pressoffice@nationwide.co.uk
www.nationwide.co.uk

NatWest
Switchboard: 020 7427 8000
Retail bank press office: 020 7672 1926
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
Press office: 020 7672 1926
ronan.kelleher@rbs.co.uk
www.rbs.co.uk

Standard Chartered
Switchboard: 020 7280 7500
Press office: 020 7280 6068
julie.smith@standardchartered.com
www.standardchartered.com/uk

Card scheme contacts

VISA International
Switchboard: 020 7937 8111
Press office: 020 7795 5336
europeanmedia@visa.com
www.visaeurope.com

MasterCard International / Maestro
Switchboard: 020 7557 5000
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
adrian.russell@citigroup.com
www.dinersclub.com

APACS, the UK payments association, is the trade body that gives banks, building societies and card issuers a forum where they can work together on non-competitive issues. 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 lead the fight against banking fraud and twice a year we publish figures on payment industry fraud losses.

To order more copies of this booklet, and for further information about card fraud and its prevention please visit www.cardwatch.org.uk.

APACS
the UK payments association

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