Financial Fraud Action UK
Working together to prevent fraud

FRAUD
THE FACTS 2010

THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD AND MEASURES TO PREVENT IT

Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud prevention, presenting a united front against financial fraud and its effects. Financial Fraud Action UK works in partnership with The UK Cards Association on industry initiatives to prevent fraud on credit and debit cards, with the Fraud Control Steering Group on non-card fraud matters and the Cheque and Credit Clearing Company on credit clearing and cheque fraud.

THE
UKCARDS
ASSOCIATION

The UK Cards Association is the leading trade association for the cards industry in the UK. With a membership that includes all major credit, debit and charge card issuers, and card acquiring banks, the role of the Association is both to unify and represent the UK card payments industry. It is responsible for formulating and implementing policy on non-competitive aspects of card payments including codes of practice, fraud prevention, major infrastructural changes, developments of standards and other matters where cross-industry benefits are identified.

"The cards industry sees fighting fraud as a key part of keeping its customers' interests centre-stage. We are committed to a wide range of measures to ensure customers feel confident, safe and secure when they use their credit and debit cards – whether in a shop, abroad, online, at a cash machine or anywhere else.

A fall in card fraud, as seen in 2009, is good news for everyone – UK consumers, retailers and the industry. We recognise that cards will always be targeted by criminals, so we are determined not only to continue to prevent, detect and deter those who are behind this type of crime, but also to make sure that innocent victims don't lose out."

MELANIE JOHNSON, Chair of The UK Cards Association, which represents UK credit and debit card providers

"Although online banking fraud losses have shown a year-on-year increase, card fraud remains a main focus of criminal activity. However, the industry remains committed to containing and reducing all areas of fraud. To this end, we will continue our partnership approach – working with law enforcement, retailers, consumers and the Home Office – to tackle fraud head-on."

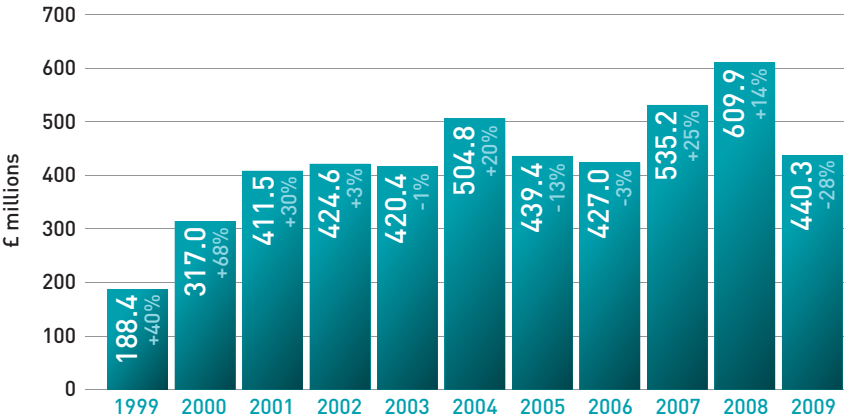
DAVID COOPER, Chairman of the Fraud Control Steering Group, the payment industry's leading non-plastic fraud prevention group

PLASTIC CARD FRAUD

06 // PLASTIC CARD FRAUD

PLASTIC CARD FRAUD LOSSES ON UK-ISSUED CARDS 1999-2009

Tinted figures show percentage change on previous year's total



ANNUAL PLASTIC CARD FRAUD LOSSES ON UK-ISSUED CARDS 1999-2009

All figures in £ millions

Fraud type	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	+/- change 08/09
Card-not-present	29.3	72.9	95.7	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	-19%
Counterfeit	50.3	107.1	160.4	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	-52%
Lost/stolen	79.7	101.9	114.0	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.9	-11%
Card ID theft	14.4	17.4	14.6	20.6	30.2	36.9	30.5	31.9	34.1	47.4	38.2	-20%
Mail non-receipt	14.6	17.7	26.8	37.1	45.1	72.9	40.0	15.4	10.2	10.2	6.9	-32%
TOTAL	188.4	317.0	411.5	424.6	420.4	504.8	439.4	427.0	535.2	609.9	440.3	-28%
Contained within this total/breakdown by location												
UK fraud	134.1	213.4	273.0	294.4	316.3	412.3	356.6	309.9	327.6	379.7	317.6	-16%
Fraud abroad	54.2	103.5	138.4	130.2	104.1	92.5	82.8	117.1	207.6	230.1	122.7	-47%

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

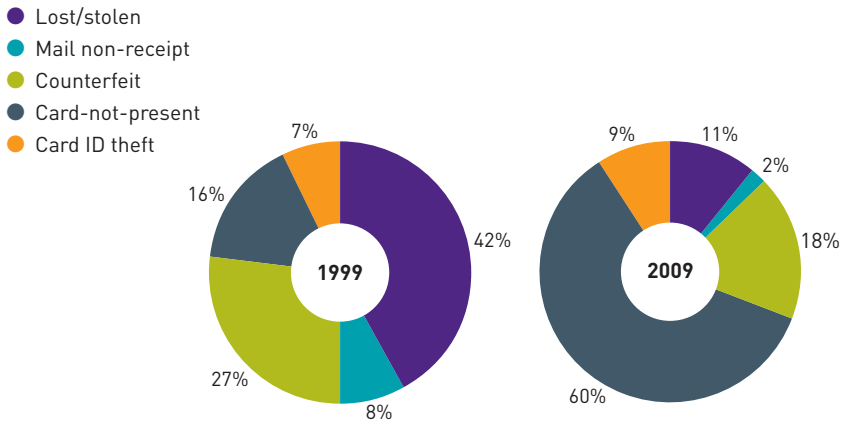
08 // PLASTIC CARD FRAUD

OVERVIEW

Total fraud losses on UK cards fell by 28% between 2008 and 2009 to £440.3 million – a decrease of £170 million on the previous year's total. This is the first time that card fraud has decreased since 2006.

Whilst card usage and transaction volumes continue to grow, card fraud losses against total turnover – at 0.091% – are still significantly less than in 2001 (before the introduction of chip and PIN) when the fraud-to-turnover ratio was more than double what it is now, at 0.183%.

CARD FRAUD LOSSES SPLIT BY TYPE (AS PERCENTAGE OF TOTAL LOSSES)



FRAUD LOSSES IN THE UK ON UK-ISSUED CARDS SPLIT BY UK REGION 2005-2009

All figures in £ millions

Region	2005	2006	2007	2008	2009	+/- change 08/09
South East	207.3	176.6	178.7	204.7	168.1	-18%
North West	33.2	35.7	35.8	42.5	38.9	-9%
East Midlands	23.8	15.0	22.8	23.8	18.9	-21%
West Midlands	20.3	17.2	24.4	23.5	22.3	-5%
Yorkshire & Humberside	27.3	27.2	24.1	22.5	18.8	-16%
South West	11.3	9.7	11.8	19.2	12.9	-33%
Scotland	13.9	9.9	11.5	18.0	11.6	-35%
North East*	7.3	6.8	7.8	10.1	10.4	+3%
East Anglia	6.2	5.4	4.8	7.6	6.1	-20%
Wales*	5.2	5.7	5.3	7.2	8.2	+13%
Northern Ireland*	0.8	0.7	0.7	0.7	1.4	+100%
UK TOTAL	356.6	309.9	327.6	379.7	317.7	-16%
Fraud abroad	82.8	117.1	207.6	230.1	122.7	-47%
TOTAL ALL UK CARDS	439.4	427.0	535.2	609.9	440.3	-28%

*The regional increases in fraud – in the North East, Wales and Northern Ireland – are due 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 mail order, phone and internet (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 location of the cardholder.

PHONE, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT OR CNP) FRAUD

£266.4 MILLION IN 2009 (DOWN 19%)

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 by mail order. The genuine cardholder may not be aware of this fraud until they check their statement.

In general, 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.

Although card-not-present fraud accounts for more than half of all card fraud losses, the past decade has seen massive growth in CNP spending, such as e-commerce.

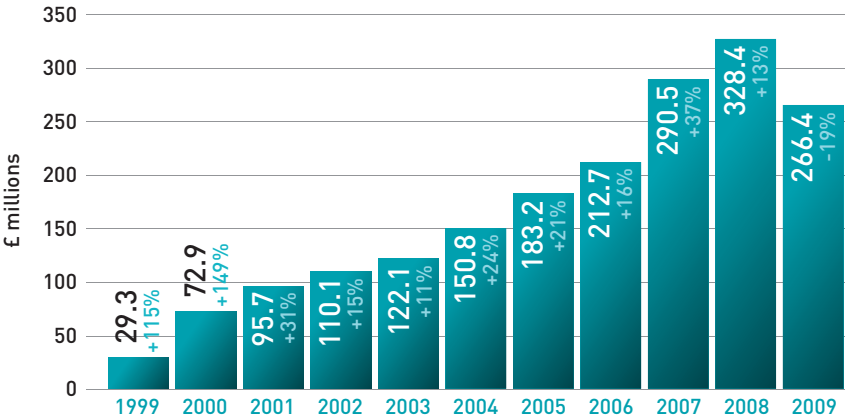
Last year saw this type of fraud showed a year-on-year decrease for the first time.

The reasons behind the decrease include the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as the continuing growth in the use of cardholder authentication processes such as MasterCard SecureCode and Verified by Visa by both online retailers and cardholders.

The industry's Be Card Smart Online campaign, launched at the end of 2008, provides consumers with straight forward practical tips to help them shop safely on the internet.

CARD-NOT-PRESENT FRAUD LOSSES ON UK-ISSUED CARDS IN 1999-2009

Tinted figures show percentage change on previous year's total



COUNTERFEIT CARD FRAUD

£80.9 MILLION IN 2009 (DOWN 52%)

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

There are several factors behind the fall in counterfeit card fraud, including:

- Increasing use by card companies of sophisticated fraud prevention software.
- The banking industry working closely with the retail community to raise awareness of the ways in which retailers can protect their chip and PIN terminals from criminal attack – minimising the opportunities for card details to be electronically copied.
- The continuing rollout of debit and credit cards with enhanced security features. Cards with an updated integrated card verification value (iCVV) have been rolled out since January 2008 and as of the end of December 2009 there were more than 106 million issued in the UK.
- The successful work of the banking industry-sponsored special police unit, the Dedicated Cheque and Plastic Crime Unit, which has prevented approximately £340 million in fraud losses in the past eight years.
- More and more countries have now introduced chip and PIN technology, which makes it much harder to use fake UK cards overseas.

16// PLASTIC CARD FRAUD

Counterfeit card fraud losses in the UK have decreased by 77% since 2004 – this is due to the fact that chip and PIN has made it much harder for criminals to use fake cards in cash machines and shops in the UK.

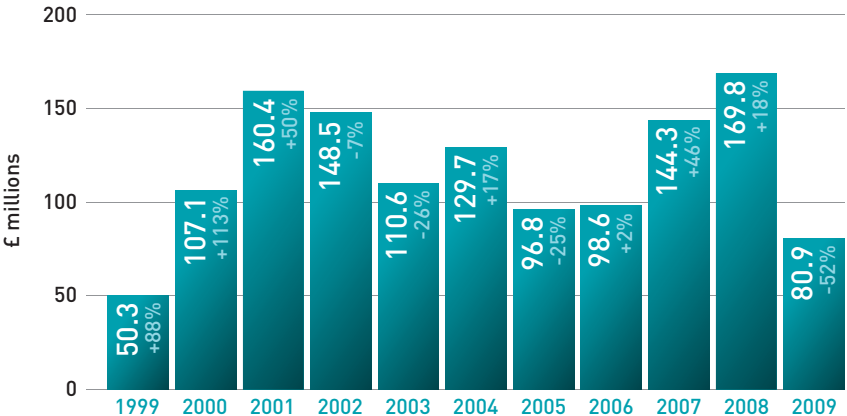
COUNTERFEIT CARD FRAUD LOSSES IN THE UK AND ABROAD 2005-2009

All figures in £ millions

Region	2005	2006	2007	2008	2009	+/- change 08/09
Domestic (in the UK)	78.6	45.8	31.0	36.2	24.5	-32%
Abroad	18.2	52.8	113.3	133.6	56.4	-59%
TOTAL	96.8	98.6	144.3	169.8	80.9	-52%

COUNTERFEIT CARD FRAUD LOSSES ON UK-ISSUED CARDS IN 1999-2009

Tinted figures show percentage change on previous year's total



LOST AND STOLEN CARD FRAUD

£47.9 MILLION IN 2009 (DOWN 11%)

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 to commit fraud via a telephone, internet or mail order transaction.

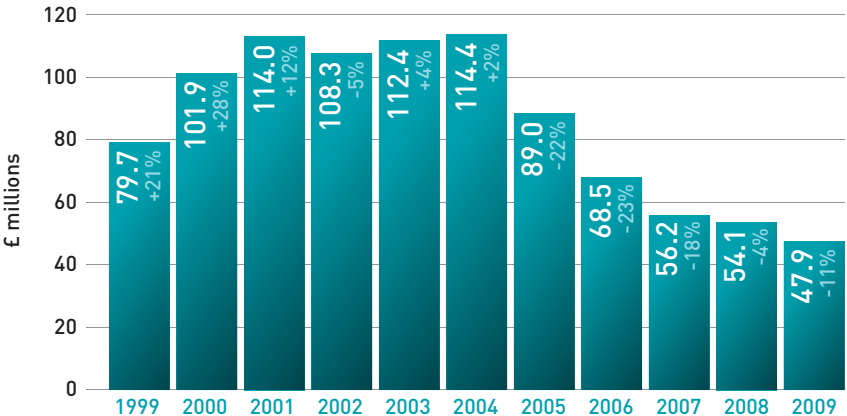
Thanks to the introduction of chip and PIN this fraud type is now at its lowest level since the industry collation of fraud losses began in 1991.

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.

LOST AND STOLEN FRAUD LOSSES ON UK-ISSUED CARDS 1999-2009

Tinted figures show percentage change on previous year's total



20// PLASTIC CARD FRAUD

CARD ID THEFT

£38.2 MILLION IN 2009 (DOWN 20%)

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.

Card ID theft fell by 20% in the past year to £38.2 million, and now accounts for just under 9% 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

£10.1 MILLION IN 2009 (DOWN 9%)

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 counterfeit documents for identification purposes.

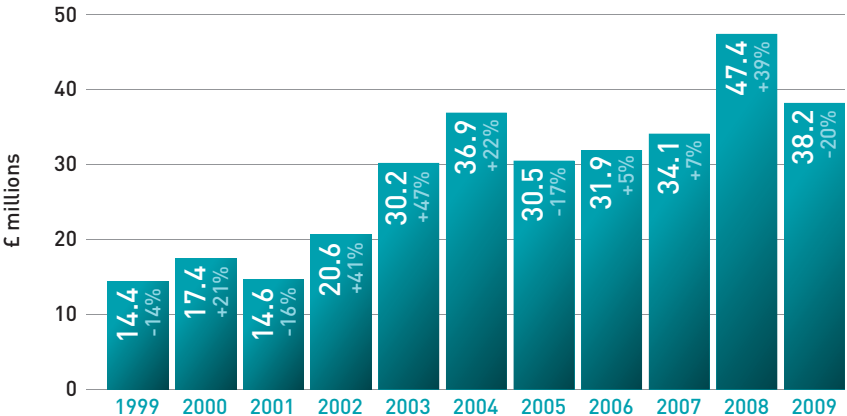
//ACCOUNT TAKEOVER

£28.1 MILLION IN 2009 (DOWN 23%)

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 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 new address.

ID THEFT ON UK-ISSUED CARDS 1999-2009

Tinted figures show percentage change on previous year's total



The decrease in both types of fraud is due to a combination of factors. The current economic climate has generally made it much more difficult for consumers to establish new lines of credit – which also impacts fraudsters. Additionally, cardholders are heeding advice to keep their personal information secure; and card companies' fraud detection systems are helping to spot and stop this type of fraud.


4907
01/05

MAIL NON-RECEIPT FRAUD

£6.9 MILLION IN 2009 (DOWN 32%)

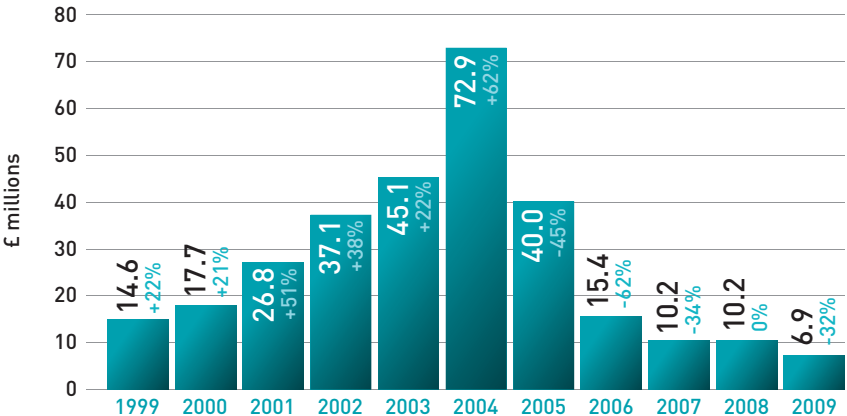
This type of fraud involves cards being stolen whilst in transit – after card companies send them out and before the genuine cardholders receive them. Properties with communal letterboxes, such as flats and student halls of residence and people who do not get their mail redirected when they change address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

Mail non-receipt fraud fell by almost a third last year to £6.9 million, and is now 91% lower than in 2004, which was the peak year for this type of fraud. The main reason behind this large decrease is because fewer cards and PINs are being sent out than in the years when all cards were being upgraded to chip and PIN. This means that there are fewer opportunities for cards to be intercepted. Even when replacement cards are issued, the cardholder already knows the PIN, so the PIN is not sent out. If a fraudster intercepts a card, he is therefore unlikely to be able to use it at a shop or cash machine in the UK.

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 use secure couriers to deliver to high-risk postcodes, or cards may be sent to a customer's branch for personal collection. Customers may also 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 1999-2009

Tinted figures show percentage change on previous year's total



WHERE DOES CARD FRAUD TAKE PLACE?

The card fraud landscape has changed mainly due to the continuing success of chip and PIN in the UK. Fraudsters are now targeting those environments that do not yet use chip and PIN, such as the internet. Overseas fraud losses have also gone down due in part to the continuing rollout of chip and PIN in other countries around the world.

UK RETAILER (FACE-TO-FACE) FRAUD

£72.1 MILLION IN 2009 (DOWN 27%)

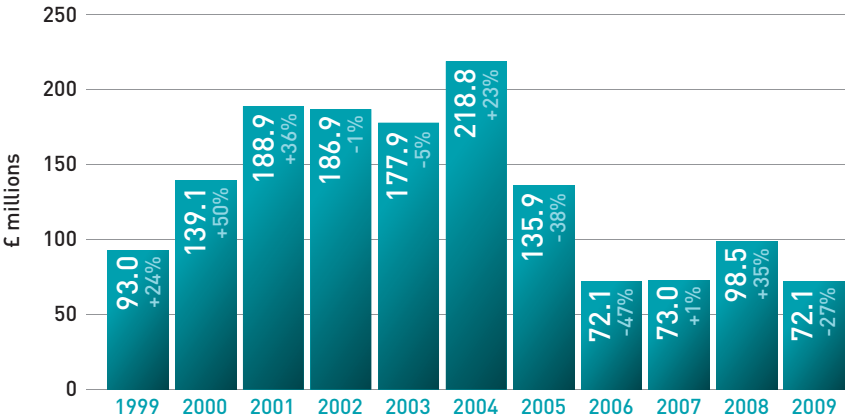
Card fraud losses in the UK high street have declined by 67% since peaking at £218.8 million in 2004.

This decrease is thanks to the success of chip and PIN. However, card fraud can still happen in shops in the UK through lost and stolen cards if a criminal has access to the PIN, for example if a cardholder has written their PIN down and stored it in the purse or wallet that is stolen.

A much smaller proportion of this fraud involves cards being used fraudulently as a result of mail non-receipt fraud, where the fraudster has been able to intercept both the card and its PIN on the way to the cardholder.

CARD FRAUD LOSSES AT UK RETAILERS (FACE-TO-FACE TRANSACTIONS) 1999-2009

Tinted figures show percentage change on previous year's total



UK CASH MACHINE FRAUD

£36.7 MILLION IN 2009 (DOWN 20%)

The amount of money withdrawn fraudulently at UK cash machines, on UK-issued cards decreased 20% last year, to £36.7 million. These losses account for just over 8% of total card fraud.

A lot of cash machine fraud is still the result of cardholders keeping their PIN written down in their purse or wallet, which is then stolen.

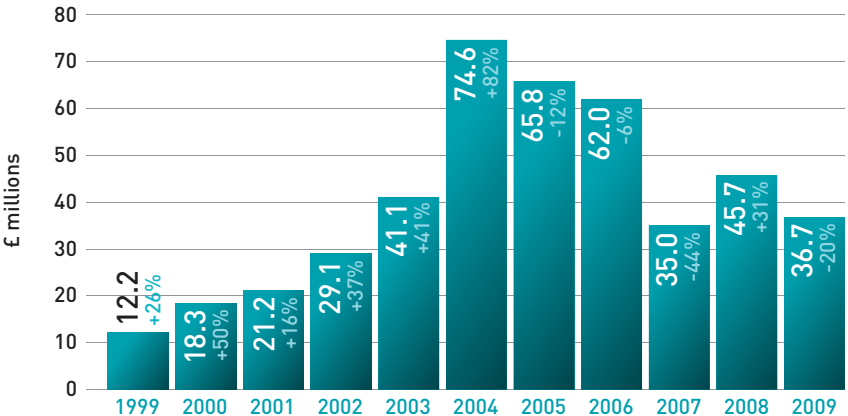
Fraudsters also use cash machines to compromise or steal cards or card details.

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

- Card-trapping devices – a device is inserted into a cash machine's card slot, which retains the card inside the cash machine. The criminal tricks the victim into re-entering their PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.
- Skimming – a 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 hidden overlooking the PIN pad to capture the PIN being entered. A fake magnetic stripe card is then produced and used with the genuine PIN to withdraw cash at cash machines overseas, where they have yet to upgrade to chip and PIN.
- Shoulder surfing – criminals watch the cardholder entering their PIN, then steal the card using distraction techniques or pickpocketing, before using the stolen card and genuine PIN.

FRAUD LOSSES AT UK CASH MACHINES 1999-2009

Tinted figures show percentage change on previous year's total



FRAUD ABROAD

£122.7 MILLION IN 2009 (DOWN 47%)

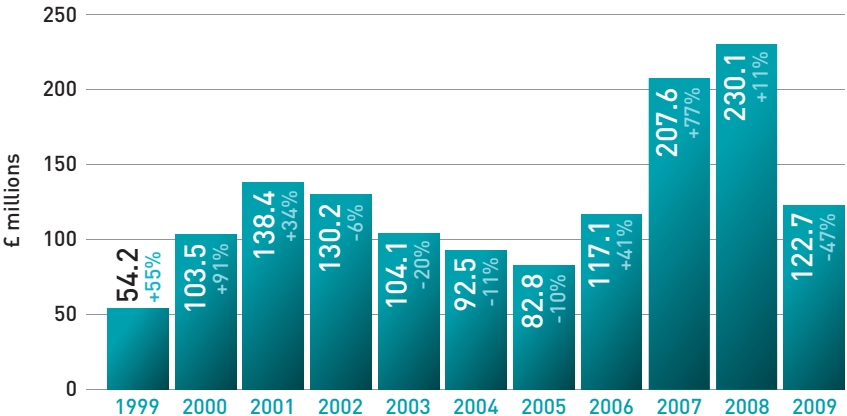
This type of fraud typically occurs as a result of criminals stealing magnetic stripe details from UK cards to make fake magnetic stripe cards for use overseas in countries yet to upgrade to chip and PIN. At £122.7 million, fraud abroad accounts for just over one quarter (28%) of total card fraud losses. However, this type of fraud fell by almost a half last year, partly due to the banks' fraud detection systems, which monitor for unusual spending patterns and stop potential fraud before it happens.

The countries where fraud is occurring on UK-issued cards have changed markedly over the past five years, since other countries – following the UK's lead – began using chip and PIN.

The proportion of total fraud abroad losses in the USA increased from 14% in 2008 to 17% in 2009. Fraud on UK-issued cards in Australia and Canada also decreased significantly – by 53% and 46% respectively – due to these countries introducing chip and PIN.

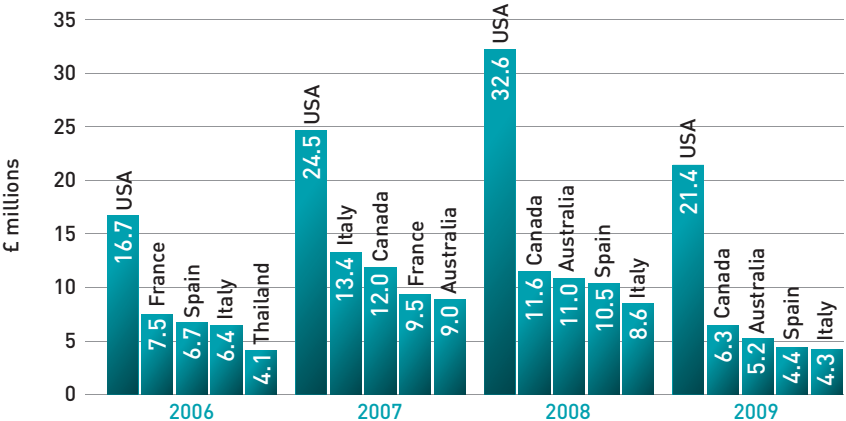
FRAUD COMMITTED ABROAD ON UK-ISSUED CARDS 1999-2009

Tinted figures show percentage change on previous year's total



TOP 5 COUNTRIES FOR FRAUD ABROAD 2006-2009

UK-issued cards or card details used fraudulently overseas



INTERNET/E-COMMERCE FRAUD ON CARDS

ESTIMATED AT £153.2 MILLION IN 2009 (DOWN 15%)

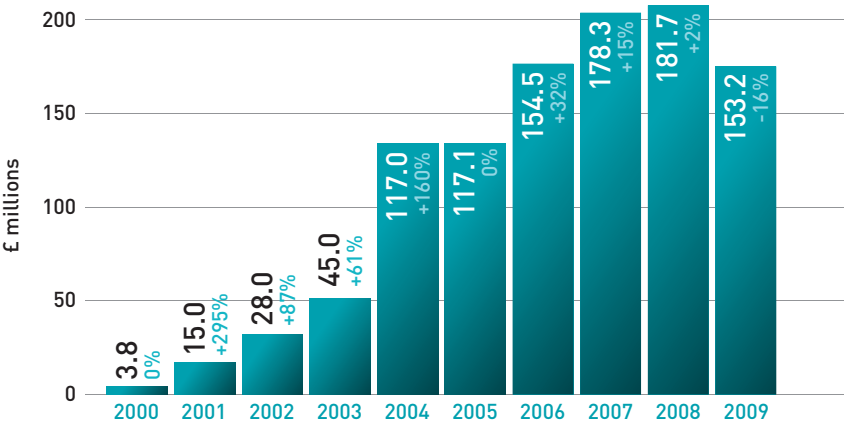
£153.2 million of card fraud took place over the internet in 2009, a decrease of 15% from 2008 when e-commerce fraud losses were £181.7 million. Internet fraud now accounts for 58% of card-not-present losses – up from 55% in 2008.

The decrease in the value of internet fraud losses has been aided by the increasing use of sophisticated fraud screening detection tools by retailers and banks to detect potential internet fraud as well as the continued growth in use of Verified by Visa and MasterCard SecureCode.

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 undertake fraudulent card-not-present transactions.

INTERNET/E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS 2000 TO 2009

Tinted figures show percentage change on previous year's total. All figures estimated.



INDUSTRY MEASURES TO PREVENT PLASTIC CARD FRAUD

CHIP AND PIN

MAKING CARD TRANSACTIONS SAFER

Chip and PIN is part of a global programme to tackle plastic card fraud and has proven to be an undoubted success, resulting in significant reductions in specific types of fraud on UK cards:

- Lost and stolen card fraud is at its lowest level for two decades.
- Counterfeit card fraud is at its lowest level since 1999.
- Fraud losses in the UK high street have fallen by 67% since 2004.
- Mail non-receipt fraud losses are at their lowest level since the industry began collating this data.

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, with 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 has been responsible for savings of approximately £340 million in estimated fraud since its launch in 2002. In 2009 the Unit had a number of successes, and achieved fraud savings in the region of £24 million.

The DCPCU is comprised of three operational teams, which are supported by an intelligence arm.

FRAUD INTELLIGENCE SHARING SYSTEM

SHARING INTELLIGENCE TO TACKLE FRAUD

A Fraud Intelligence Sharing System (FISS) was established in 2008 which enables 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.

NATIONAL FRAUD INTELLIGENCE BUREAU

The payments industry has worked with the City of London Police to establish the National Fraud Intelligence Bureau (NFIB).

This intelligence sharing initiative should provide a better vehicle for relevant organisations to work together to tackle fraud. Confirmed fraud data from the payment industry's existing and successful Fraud Intelligence Sharing System will feed into the NFIB.

INDUSTRY HOT CARD FILE (IHCF)

CHECKING TRANSACTIONS FOR CARDS BEING USED FRAUDULENTLY

The IHCF contains information on more than 6 million cards reported lost or stolen. During the last year, over 434,756 (491,990 in 2008) cases of attempted fraud were prevented by this system. The IHCF is also used successfully at French motorway tollbooths to combat the use of stolen UK cards at road tolls.

More than 60,000 UK 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.

CIFAS – THE UK'S FRAUD PREVENTION SERVICE

SHARING INFORMATION TO STOP FRAUD

CIFAS is the UK's Fraud Prevention Service with 265 members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, telecommunications, factoring and share dealing. Members share information about identified frauds.

For more information visit **www.cifas.org.uk**.

REDUCING PHONE, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT) FRAUD

HELPING BUSINESSES FIGHT CNP FRAUD

Although phone, internet and mail order fraud decreased in 2009, losses still account for more than half of all card fraud. However, the fall in this type of fraud is all the more notable given the continuing popularity of shopping over the phone and the internet. Indeed, the estimated total value of internet spending in 2009 was £47.2 billion – an increase of 15% on the previous year (£41.2 billion in 2008). A number of initiatives are in place to tackle phone, internet and mail order fraud:

- Verified by Visa and MasterCard SecureCode are online fraud prevention solutions that make cards more secure when shopping online. Cardholders are prompted to register with Verified by Visa or 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. More than 64 million cards – 43% of all UK cards – had already been registered by March 2010 (up from 37 million in December 2008). More information can be found at **www.becardsmart.org.uk**.

- An automated cardholder address verification (AVS) and card security code (CSC) system is available for businesses that accept phone, internet or 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.
- The industry encourages retailers 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.financialfraudaction.org.uk**.

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

Although card ID theft decreased by 20% in 2009 and remains a relatively small proportion of total card fraud losses – just under 9% – the industry remains committed to enhancing existing prevention measures and developing new ways of combating this type of fraud.

The banking industry is represented on the Identity Fraud Communications and Awareness Group (IFCAG) which includes representatives from the British Bankers' Association and CIFAS, amongst many others. It has created a website for identity fraud prevention at **www.identitytheft.org.uk**, which provides best practice guidelines for businesses that could be targeted by identity

fraudsters. There is also 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 site also advises the public how best to protect themselves from becoming a victim of identity theft and what to do if they have. This is complemented with a range of leaflets and posters for use in public areas such as libraries, citizens advice bureaux and bank counters.

For more information visit **www.identitytheft.org.uk**.

INDUSTRY MEASURES TO PREVENT CASH MACHINE CRIME

MULTI-LAYERED APPROACH TO TACKLING FRAUD

Although UK cash machine fraud losses have decreased by 51% since 2004 – the peak year for this type of fraud – the UK banking industry continues to work with cash machine suppliers to enhance technical solutions to prevent cash machine tampering. The industry also works 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:

- Technology upgrades to make cash machines tamper-proof, such as redesigned card reader surrounds in order to make it difficult for fraudsters to attach a skimming device to a machine.

- Privacy spaces, which comprise a zoned area marked on the ground in front of the cash machine to enable users to withdraw cash more safely.
- Consumer advice on best practice when using a cash machine. This includes co-ordinated use of screen messages designed to raise cash machine users' awareness of security.
- Encouraging regular inspections of cash machines by cash machine owners for evidence of tampering and unusual attachments.
- Use of CCTV to deter criminal activity.
- LINK, the UK's cash machine network, works in partnership with independent charity, Crimestoppers to offer rewards of up to £25,000 for information relating to cash machine crime. Anyone with details about those responsible for cash machine crime – such as card skimming or even physical attacks on the machine itself – can call Crimestoppers on 0800 555 111, where they can leave their information completely anonymously.

CHEQUE FRAUD

CHEQUE FRAUD

£29.8 MILLION IN 2009 (DOWN 29%)

Following year-on-year increases in 2007 and 2008, last year saw a 29% drop in cheque fraud losses.

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

TYPES OF CHEQUE FRAUD

//COUNTERFEIT CHEQUE FRAUD

£4.7 MILLION IN 2009 (DOWN 38%)

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

£15.7 MILLION IN 2009 (DOWN 10%)

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

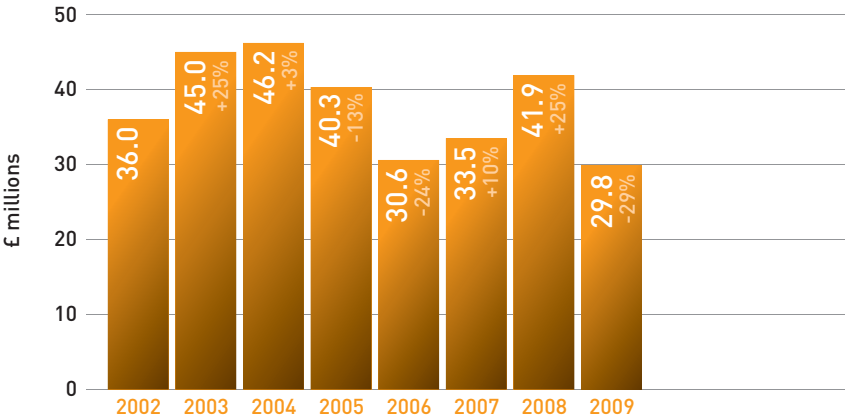
//FRAUDULENTLY ALTERED CHEQUES

£9.3 MILLION IN 2009 (DOWN 45%)

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

CHEQUE FRAUD LOSSES 2002-2009

Tinted figures show percentage change on previous year's total



COMMON CHEQUE SCAMS

There are a number of scams involving cheques. 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.

Over recent years organised gangs have particularly targeted consumers selling high-value goods such as cars, by offering to pay using stolen or counterfeit cheques and bankers' drafts. Anyone wanting to accept a cheque or banker's draft 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 working day after they have paid the cheque into their account).

Frequently this scam will also involve 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.

In this type of scam the seller is 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 banker's draft is fraudulent. 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 (see 2-4-6 clearing timescales on next page).

WHAT IS THE BANKING INDUSTRY DOING TO PROTECT CUSTOMERS FROM CHEQUE FRAUD?

In November 2007, the banking industry introduced changes known as 2-4-6 to cheque clearing timescales to help protect customers who inadvertently accept cheques from fraudsters. 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. Subsequently 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.

WHAT IS THE BANKING INDUSTRY DOING TO PREVENT CHEQUE FRAUD?

There is a range of prevention measures 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. This approach is very successful and in the past year the banking industry successfully identified close to 90% of all fraudulent cheques as they went through the cheque clearing process. However, fraudsters are always on the lookout for new scams.

Another way in which the industry is combating cheque fraud is through the Cheque Printer Accreditation Scheme (CPAS), which was set up in 1995 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. Customers' chequebooks are printed by CPAS members.

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 AND PHONE BANKING FRAUD

54// ONLINE AND PHONE BANKING FRAUD

ONLINE BANKING FRAUD

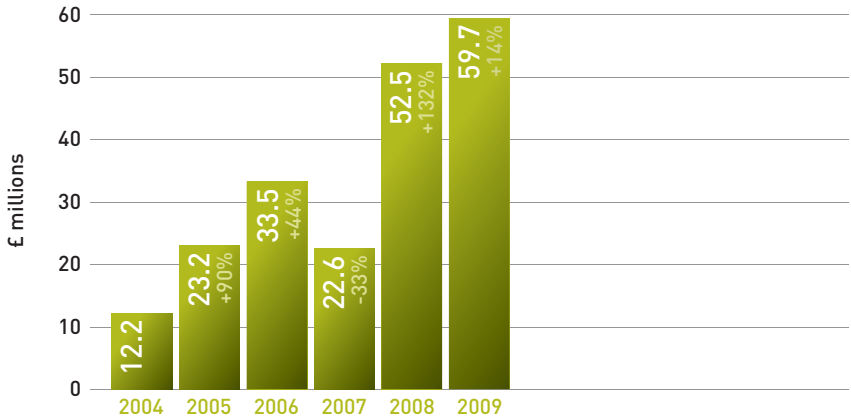
£59.7 MILLION IN 2009 (UP 14%)

In 2009 online banking fraud losses totalled £59.7 million – an increase of 14% from the previous year (£52.5 million in 2008).

This increase is due to a number of factors. As well as an increase in phishing incidents, online banking customers are increasingly being targeted by malware (malicious software) attacks. These increases have also gone hand in hand with a rise in the number of people banking online. The Police Central e-Crime Unit (PCeU), which launched in spring 2009, is helping to tackle these losses by providing specialist police officer training and co-ordinating cross-force initiatives to crack down on online offences. The PCeU also works with the national fraud reporting centre Action Fraud and supports the development of the police response to e-crime across the country.

ONLINE BANKING FRAUD LOSSES 2004-2009

Tinted figures show percentage change on previous year's total



56// ONLINE AND PHONE BANKING FRAUD

COMMON SCAMS

Scams such as phishing and malware 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 such as a bank, 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.

//MALWARE (MALICIOUS SOFTWARE)

Online banking customers are increasingly being targeted by malware attacks.

Malware includes computer viruses that can be installed on a computer without the user's knowledge, typically by users clicking on a link in an unsolicited email, or by downloading suspicious software. Malware is capable of logging keystrokes thereby capturing passwords and other financial information.

NUMBER OF PHISHING WEBSITES* TARGETED AGAINST UK BANKS AND BUILDING SOCIETIES BY MONTH 2005-2009

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	51,161
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	43,991
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	25,797
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	14,156
2005	18	29	27	54	72	122	153	160	190	267	255	353	1,700

* 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.

//MONEY MULES

Most of the fraudsters behind online banking scams are located overseas, so 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 online scams. Some mules are recruited under false pretences, in the belief that they will be working 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.

Money mules are recruited by a variety of methods, including spam emails, adverts on genuine recruitment websites or newspapers, and approaches to people with their CVs displayed online. There were 1,220 money mule recruitment advertisements recorded in 2009, compared with 1,623 in 2008.

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 are the easiest part of the chain to track down.

NUMBER OF MULE RECRUITMENT ADVERTS* BY MONTH 2005-2009

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2009	107	56	118	77	73	128	139	94	98	118	117	95	1,220
2008	161	232	110	121	134	115	159	166	125	94	90	116	1,623
2007	77	128	144	99	91	116	123	142	148	110	163	121	1,462
2006	42	64	96	81	110	75	72	109	109	132	113	84	1,087
2005	21	29	28	33	44	41	26	41	40	57	59	53	473

* These are calculated by recording 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, the Police Central e-Crime Unit (PCeU), overseas law enforcement agencies, technology companies, anti-virus firms and Internet Service Providers.

A number of initiatives are already in place:

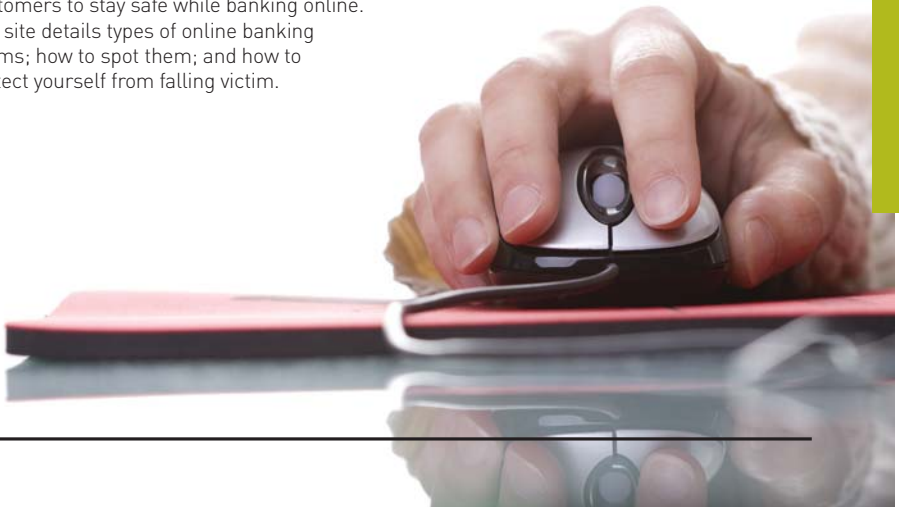
- Monitoring of the internet at industry and bank level to detect and close down phishing-related websites.
- Two-way communication with online partners so security intelligence can be shared and used effectively.
- Development and use of clear and consistent advice for consumers.
- Banks continually monitor for potentially fraudulent online and phone banking transactions and will contact a customer to check if a suspect transaction is genuine or not.

One of the initiatives introduced by some banks to provide a higher level of online banking security is 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 entering the PIN, the card reader generates a unique, one-time only passcode, which the cardholder provides, when prompted during a transaction, 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.

The industry has also created **www.banksafeonline.org.uk** to help customers to stay safe while banking online. The site details types of online banking scams; how to spot them; and how to protect yourself from falling victim.



PHONE BANKING FRAUD

£12.1 MILLION IN 2009

2009 was the first year that phone banking fraud losses were collated centrally – previously these figures were only quantified by banks on an individual basis. Producing an industry-wide figure will enable the industry to understand and help prevent this emerging crime.

//HOW DOES PHONE BANKING FRAUD HAPPEN?

In many cases, a fraudster uses identity theft techniques to steal personal details about an intended victim, including their phone number. The fraudster then calls the victim – pretends to be a representative of their bank – and uses a pretext such as asking the victim to 're-confirm' their security credentials to get hold of sensitive information including complete passwords. This then enables them to access the victim's account.

//WHAT IS THE INDUSTRY DOING TO TACKLE THIS TYPE OF FRAUD?

Individually, all banks have sophisticated security systems in place to protect their customers' accounts, and are constantly working to improve them. Collectively, the banking industry shares intelligence and information on this type of fraud and liaises with law enforcement, the telecommunications industry and other key stakeholders in order to further improve the security of telephone-based services, and to identify and prosecute the perpetrators.

FACTS AND FIGURES 2009

PLASTIC CARDS

- There were 143.7 million payment cards in issue in the UK at the end of 2009, which included:
  - 79.3 million debit cards
  - 58.1 million credit cards and 6.4 million charge cards
- Over 11.0 billion transactions were made on UK cards in 2009, to a total value of £620 billion.
- The average number of cards per person in 2009 was 3.6.
- Spending on plastic cards in the UK amounted to £396 billion last year, which comprised £264 billion on debit cards, and £132 billion on credit and charge cards.
- Internet card spending has risen by almost 200% over the last five years to £55.6 billion in 2009.

CASH MACHINES

- There were 62,192 cash machines in the UK at the end of 2009.
- There were 2.9 billion cash withdrawals from cash machines in the UK last year – an average of 92 per second.
- The total value withdrawn from cash machines in the UK was £192.8 billion in 2009 – an average of £6,114 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 3.5 million business and personal cheques issued each day in 2009, compared with 11 million in the peak year for cheque volumes, 1990.
- In 2009, adults received fewer than five cheques on average per year.
- The average value of a personal cheque transaction in 2009 was £268.
- Only 4 million adults still used guaranteed cheques on a regular basis in 2009, compared with 15 million in 1996.
- Only 2% of retail spending is still paid by cheque, compared with over 60% by debit or credit card.

ONLINE BANKING

- Over 24 million adults banked online in 2009.
- 53% of internet users bank online.
- Use is highest among 35 to 44 year olds, 60% of which access at least one account online.
- 99% of online banking users access their main current account.

CONTACTS AND WEBSITES

WEB LINKS

www.actionfraud.org.uk
The UK's national fraud reporting centre – a central point of contact for victims of fraud.

www.attorneygeneral.gov.uk
The National Fraud Authority has been established by the Attorney General's Office as the body to lead on the delivery of the UK's first National Fraud Strategy.

www.banksafeonline.org.uk
Advise for online banking users, to help protect themselves from fraud.

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

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

www.chequeandcredit.co.uk
The Cheque and Credit Clearing Company manages the cheque and paper credit clearing systems in Great Britain. Its main objective is to ensure the integrity and efficiency of these systems. It also manages the Cheque Printer Accreditation Scheme (CPAS).

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.crimestoppers-uk.org
Crimestoppers is an independent charity helping to find criminals and help fight crime.

www.dcpcu.org.uk
Explains how the banking-sponsored special police squad, the 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.financialfraudaction.org.uk
Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud, presenting a united front against financial fraud and its effects.

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 or your business from identity theft, what to do if it happens to you and suggestions on where to get further help.

www.link.co.uk
LINK is the UK's cash machine (ATM) network.

70// CONTACTS AND WEBSITES

www.paymentscouncil.org.uk
The strategic payments body set up to ensure that UK payments plans and services meet the needs of users, payment service providers and the wider economy.

www.theukcardsassociation.org.uk
The UK Cards Association is the leading trade association for the card payments industry in the UK.

PUBLICATIONS

//UK PAYMENT STATISTICS 2010

An annual publication that provides a comprehensive source of UK payment statistics and historical data from 1999 to 2009, with additional forecast data up to and including 2017. £750.
(Publication date: June 2010)

//UK CASH AND CASH MACHINES 2010

Examines the main trends in cash payments, the deployment and usage of cash machines, and other forms of cash acquisition. £250.
(Publication date: May 2010)

//UK PLASTIC CARDS 2010

Details trends in the use of plastic payment cards in the UK by businesses and individuals. £250.
(Publication date: May 2010)

//UK CHEQUES 2010

Examines the main trends in the use of cheques for payment and cash acquisition. £250.
(Publication date: September 2010)

//UK AUTOMATED PAYMENTS 2010

Looks at the main trends in the use of direct credits, Direct Debits, Faster Payments, standing orders and CHAPS payments. £250.
(Publication date: August 2010)

//UK CONSUMER PAYMENTS 2010

Looks in detail at consumer holdings and use of different payment methods. £1,500.
(Publication date: October 2010)

For more information or to order any of these publications please contact press@ukpayments.org.uk.

FRAUD PREVENTION MATERIALS

//DON'T REWARD FRAUD

A guide for consumers detailing the ways in which fraudsters operate, and useful advice on how to avoid being a victim of fraud.

//SECURITY GUIDANCE FOR CARD ACCEPTANCE DEVICES DEPLOYED IN THE FACE TO FACE ENVIRONMENT

These guidelines are for retailers accepting face-to-face card payments. They are designed to complement card industry rules and regulations and advice given by point-of-sale solution providers (including banks and third party suppliers).

For more information about fraud prevention materials please visit **www.financialfraudaction.org.uk**.

USEFUL CONTACTS

// PAYMENTS INDUSTRY PRESS OFFICE

(CHAPS, Cheque & Credit Clearing Company, DCPCU, Faster Payments, FFA, LINK, Payments Council, The UK Cards Association and SWIFT)
020 3217 8316
press@ukpayments.org.uk

Sandra Quinn, Director of communications
020 3217 8234
M: 07768 044656
sandra.quinn@ukpayments.org.uk

Jemma Smith, Head of PR
020 3217 8340
M: 07811 113075
jemma.smith@ukpayments.org.uk

Mark Bowerman, PR manager
020 3217 8251
M: 07799 627256
mark.bowerman@ukpayments.org.uk

Michelle Whiteman, Press officer
020 3217 8316
M: 07947 217687
michelle.whiteman@ukpayments.org.uk

Doriena Koldenhof, PR assistant
020 3217 8368
doriena.koldenhof@ukpayments.org.uk

Rosalind Beaumont, Public affairs manager
020 3217 8280
rosalind.beaumont@ukpayments.org.uk

// BRITISH BANKERS' ASSOCIATION
020 7216 8800

// BUILDING SOCIETIES ASSOCIATION
020 7520 5900

// CIFAS – THE UK'S FRAUD PREVENTION SERVICE
033 0100 0180

// CREDIT REFERENCE AGENCIES
Call Credit: 0870 060 1414
Equifax: 0870 010 0583
Experian: 0870 241 6212

// FINANCIAL OMBUDSMAN SERVICE
0845 080 1800

// FSA
Consumer helpline: 0300 500 5000
Press office: 020 7066 3232
press.office@fsa.gov.uk
www.fsa.gov.uk

// LENDING STANDARDS BOARD
020 7012 0085

// ROYAL MAIL CUSTOMER ENQUIRIES
0845 7740 740

PRESS OFFICE CONTACTS

// ALLIANCE & LEICESTER
Switchboard: 0116 201 1000
Press office: See Santander
www.alliance-leicester-group.co.uk

// AMERICAN EXPRESS
Switchboard: 0127 3693 555
Press office: 0127 3216 674
jacquie.goozee@aexp.com
www.americanexpress.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: 020 3201 6000
Press office: 020 3201 6509
sandra.grandison@boiuk.com
www.bank-of-ireland.co.uk

// BANK OF TOKYO-MITSUBISHI
Switchboard: 020 7588 1111
www.uk.bk.mufg.jp

// 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
teresa.juliet.lathangue@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

// CO-OPERATIVE BANK
Switchboard: 0161 832 3456
Press office: 0161 903 3808 / 3833
duncan.bowker@cfs.coop
www.co-operativebank.co.uk

// COVENTRY BUILDING SOCIETY
Switchboard: 0845 766 5522
Press office: 0870 607 7727
media.coventrybuildingsociety@btconnect.com
www.coventrybuildingsociety.co.uk

// DINERS CLUB
Switchboard: 0870 190 0011
Press office: 0870 190 0011
www.dinersclub.com

// EGG
Switchboard: 01338 395 919
Press office: 0207 508 7355
prteam@egg.com
www.egg.com

// ELAVON
Switchboard: 0845 8500195
holly.lytle@elavon.com
www.elavonms.com

// HSBC/FIRST DIRECT
Switchboard: 020 7991 8888
Press office: 020 7991 0641
pressoffice@hsbc.com
www.hsbc.com

// JP MORGAN
Switchboard: 020 7742 6000
Press office: 020 7742 6326
jane.e.drew@jpmorgan.com
www.jpmorgan.com

// LLOYDS BANKING GROUP
(HBOS, Lloyds TSB, & Halifax)
Switchboard: 020 7626 1500
Press office: 0207 356 2374
mark.elliott2@lloydsbanking.com
www.lloydsbankinggroup.com/

// MASTERCARD INTERNATIONAL/MAESTRO
Switchboard: 020 7557 5000
Press office: 0844 875 1522
mastercardpressoffice@webershandwick.com
www.mastercard.com/uk

// MBNA EUROPE BANK
Switchboard: 01244 672 000
Press office: 020 7174 4441
elizabeth.wood@bankofamerica.com
www.mbna.com

// NATIONWIDE
Switchboard: 01793 655 000
Press office: 01793 655 198
press.office@nationwide.co.uk
www.nationwide.co.uk

// NORTHERN BANK
Switchboard: 028 9024 5277
Press office: 028 9004 8656
rhonda.gibson@northernbank.co.uk
www.northernbank.co.uk

// RBS GROUP
(RBS & NatWest)
Switchboard: 0131 556 8555
Press office: 0131 523 4205
www.natwest.com
www.rbs.co.uk

//SANTANDER (ALLIANCE & LEICESTER)
Switchboard: 0870 607 6000
Press office: 020 7756 4212
andy.g.smith@santander.co.uk
www.santander.co.uk

//TESCO PERSONAL FINANCE
Switchboard: 0131 479 1000
Press office: 0131 479 1345
press.office@tescopf.com
www.tescofinance.com

//VANQUIS BANK
(via Provident Financial)
Press office: 01274 731111
Annette.Stewart@providentfinancial.com
www.vanquis.co.uk

//VISA INTERNATIONAL
Switchboard: 020 7795 5777
Press office: 020 7795 5336
europeanmedia@visa.com
www.visaeurope.com

This document is provided for information purposes only. While every effort is made to ensure the accuracy of any information or other material contained in this document, it is provided on the basis that UK Payments Administration Ltd (and its members, either individually or collectively) accept no responsibility for any loss, damage, cost or expense of whatsoever kind arising directly or indirectly from, or in connection with, the use by any person of any information or other material contained therein. Any use of the information or other material contained in this document shall signify agreement to this provision.

© UK Payments Administration Ltd 2010 Published by the UK Payments Administration

Recycled
Supporting responsible use of forest resources
www.fsc.org Cert no. SA-COC-002209
© 1996 Forest Stewardship Council

Printed on paper made from well managed sources containing 75% recycled chlorine free material. Cover laminated with Cellogreen which is sustainable, compostable and recyclable.

BWC 2702 06/10

Financial Fraud Action UK
Working together to prevent fraud

Supported by

THE UKCARDS ASSOCIATION

Cheque & Credit Clearing Company

Mercury House, Triton Court, 14 Finsbury Square, London, EC2A 1LQ
2 Thomas More Square, London, E1W 1YN (after 10 July 2010)