



Financial Fraud Action UK
Working together to prevent fraud



THE
UKCARDS
ASSOCIATION

ADDRESS

2 Thomas More Square
London
E1W 1YN

WEBSITE

www.financialfraudaction.org.uk

DIRECT LINE

020 3217 8251

EMAIL

press@ukpayments.org.uk

PRESS RELEASE

Embargoed: Not for release before 00:01am Wednesday 5 October 2011

Card fraud and online banking fraud losses fall, but cheque fraud and phone banking fraud losses rise

- **Fraudsters return to low-tech scams as initiatives continue to drive down fraud**
- **Industry reminds customers of top tips to help avoid the common scams**

New figures released today (5 October 2011) show that fraud losses on UK cards decreased in the first half of 2011 compared with the same time last year, as did fraud on online bank accounts. However, cheque fraud and fraud on phone banking accounts increased over the same period.

Total fraud losses on UK cards fell to £169.8 million between January and June 2011 – a 9 per cent reduction compared with losses in the first half of 2010. This half-year total is the lowest for eleven years and also the third consecutive decrease. The sustained fall is due to the success of a number of industry initiatives such as the increasing use of fraud detection software, the roll-out of updated chip cards and the increasing roll-out of chip and PIN technology abroad. Lost and stolen card fraud losses rose slightly, increasing by £4.4 million. Initiatives such as chip and PIN have made it harder to commit ‘high-tech’ frauds, and criminals are instead reverting to more basic frauds centred around stealing people’s cards and PINs. These scams range from distracting people in shops or at cash machines and then stealing their cards without them noticing, to simply tricking them into handing over their cards and PINs on their own doorstep¹.

Online banking fraud losses totalled £16.9 million during January to June 2011 – a 32 per cent fall on the 2010 half-year figure. A variety of factors have contributed to the decrease in online banking fraud, including increased customer awareness of computer security combined with banks’ use of fraud detection software. However, **phone banking fraud losses rose to £8.6 million** (a 48 per cent increase) during January to June 2011. As with card fraud, criminals are focusing on the straightforward crime of duping a customer into believing they are dealing with a bank or police representative and getting them to disclose their financial security details – such as PINs, passwords and login details - which the criminal then uses to access the customer’s bank account over the phone.

Cheque fraud losses increased from £14.0 million in the first half of 2010 to **£16.4 million** during the same period in 2011. Although this is a 17 per cent increase, the overwhelming majority of this type of fraud is stopped before the cheque is paid. In fact, more than £254 million of attempted cheque fraud was spotted and stopped during the clearing process in the first half of this year.

Fraud figures released by the National Fraud Authority (NFA) earlier in the year serve to put these banking fraud losses into perspective. The NFA estimated that fraud in all its guises costs the UK more than £38 billion a year – card and banking fraud accounts for only 1.2 per cent of this figure. Furthermore, in the UK - unlike many other countries outside Europe - innocent victims of any type of payment fraud on their debit or credit card or account are protected and should not suffer any financial loss.

...more

DCI Paul Barnard, Head of the Dedicated Cheque and Plastic Crime Unit (DCPCU), the special police squad which is sponsored by the banking industry and has an ongoing brief to help stamp out organised payment fraud across the UK, said:

"Losses are appreciably lower than they were a few years ago and everyone involved in tackling fraud has reason to be encouraged by this – and that includes bank customers who, as their own front-line of defence, have certainly played their part too.

"However, there has been an increase in old fashioned scams – criminals using distraction techniques and social engineering methods to get hold of people's cards or phone banking details. We are urging everyone to be on their guard. Your bank or the police will never cold call you or email you and ask you for your login details, cards or PINs. If anyone does, they are probably a criminal, so hang up the phone or delete the email."

Half-yearly plastic card fraud losses on UK-issued cards January to June 2007 to January to June 2011

Card Fraud Type – on UK issued credit and debit cards	Jan-June 2007	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	+/- 10/11
Phone, internet and mail order fraud (Card-not-present fraud)	£137.0m	£163.9m	£134.0m	£118.2m	£109.2m	-8%
Counterfeit (skimmed/cloned) fraud	£72.3m	£88.8m	£46.3m	£28.2m	£18.0m	-36%
Fraud on lost or stolen cards	£30.7m	£26.8m	£25.1m	£21.3m	£25.7m	+20%
Card ID theft	£18.7m	£19.5m	£23.9m	£15.0m	£11.5m	-23%
Mail non-receipt	£4.9m	£5.3m	£3.5m	£3.8m	£5.4m	+42%
TOTAL	£263.6m	£304.2m	£232.8m	£186.8m	£169.8m	-9%
Contained within this total:						
UK retail face-to-face transactions	£37.5m	£47.3m	£34.7m	£33.8m	£22.3m	-34%
UK cash machine fraud	£17.1m	£20.9m	£20.3m	£17.0m	£15.2m	-11%
Domestic/International split of total:						
UK fraud	£154.8m	£181.8m	£165.6m	£135.2m	£130.4m	-4%
Fraud abroad	£108.8m	£122.4m	£67.1m	£51.5m	£39.4m	-24%

Cheque fraud losses January to June 2007 to January to June 2011

	Jan-June 2007	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	+/- 10/11
Cheque fraud	£15.1m	£21.2m	£15.6m	£14.0m	£16.4m	+17%

Half-yearly remote (online and phone) banking fraud losses January to June 2009 to January to June 2011

	Jan-June 2007	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	+/- 10/11
Online banking fraud losses	£7.5m	£25.2m	£39.0m	£24.9m	£16.9m	-32%
Phone banking fraud losses	-	-	£5.3m	£5.8m	£8.6m	+48%
Remote banking fraud losses	-	-	£44.3m	£30.7m	£25.5m	-17%

Online banking fraud: No. of phishing websites	7,224	20,682	26,045	31,448	37,198	+/- +18%
---	-------	--------	--------	--------	--------	-------------

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

...more

Consumers can significantly reduce the chances of being a victim of fraud by following these top tips:

- i) Ensure you are the only person who knows your PIN. Your bank or the police will never phone or email you and ask you to disclose it.
- ii) Your bank will never ring you and tell you that they are coming around to pick up your card, so never hand it over to anyone who comes to 'collect it'.
- iii) Shield your PIN with your free hand when typing it into a keypad in a shop or at a cash machine.
- iv) Only shop on secure websites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser.
- v) Rip up or preferably shred statements, receipts and documents that contain information relating to your financial affairs when you dispose of them.
- vi) Never accept a cheque from someone unless you know and trust them, especially if the cheque is for a high value.
- vii) When writing a cheque make sure you draw a line through all unused space on the payee line and the amount line to help prevent the cheque being fraudulently altered.
- viii) Make sure you have up-to-date anti-virus software installed on your computer.

ENDS

For further information contact the press office on 020 3217 8251/ 020 3217 8441/ 020 3217 8340.

Notes to editors:

1 A typical social engineering scam begins with a fraudster phoning up, typically claiming to be from the prospective victim's bank, and saying either that their systems have flagged up a fraudulent transaction on their card or that their card is due to expire and needs replacing. By seeming to offer assistance, the fraudster tries to gain the victim's trust. In most cases the victim is then asked to 'activate' or 'authorise' the replacement card in advance by keying their PIN into their phone's handset. The fraudster uses the audio tones from the keypad entries to decipher the victim's PIN.

The fraudster or an accomplice then poses as a bank representative or a courier to pick up the customer's card from them at their home, sometimes also giving the victim a replacement card (which is a fake). In some cases a genuine courier company is hired to pick up the card, which the victim has been asked to place in an envelope. Once they have the victim's card and the PIN the fraudster uses them to withdraw cash and go on a spending spree.

2 There is no one single reason for the drop in card fraud, rather it is the result of a number of initiatives including:

- The increasing use of sophisticated fraud screening detection tools by retailers and banks, which is helping to tackle phone, internet and mail order fraud (card-not-present fraud). Additionally, the continuing growth in the use of *MasterCard SecureCode*, *Verified by Visa* and *American Express SafeKey* (online fraud prevention solutions that make cards more secure when online shopping), by both online retailers and cardholders is a contributory factor.
- The work of the Dedicated Cheque and Plastic Crime Unit (DCPCU) – the industry-sponsored special police unit, has proven highly successful. Figures show that it has been responsible for keeping more than £370 million of customers' money out of criminal hands since its launch in 2002.
- The card industry continues to work closely with the retail community to raise awareness of the ways in which retailers can protect their chip and PIN equipment from criminal attack.
- Increasing numbers of retailers are also implementing the cardholder data protection processes required of them through the Payment Card Industry Data Security Standard (PCI DSS).
- Fraud abroad losses have fallen by more than two-thirds in the past three years. One of the factors causing this is the fraud detection systems used by the banks and card companies, which monitor for unusual spending - meaning that potential fraud is stopped before it happens. The increasing rollout of chip and PIN in more and more countries around the world also makes

it harder for criminals to commit counterfeit card fraud.

- Continued investment by cash machine owners in technical defences to help prevent criminals from copying or skimming the magnetic stripe details from genuine cards.
- Cards with an updated integrated circuit card verification value (iCVV) have been rolled out since 1 January 2008. These cards - there are now 135 million of these cards in issue (as at 31 March 2011) - help tackle the type of fraud seen where fraudsters tamper with chip and PIN terminals to harvest card details. If an iCVV card was compromised in this way, the data would be useless to the fraudster (i.e. a fake magnetic stripe card created via a compromise of this type would not work overseas in a non-chip and PIN country). Issuers are also rolling out Dynamic Data Authentication (DDA) cards and (as at 31 March 2011) there were 74 million of these in issue.

3 The UK Cards Association is the leading trade association for the card payments industry in the UK. With a membership that includes all major credit, debit and charge card issuers, and card payment acquirers, the Association advances industry best practice, contributes to the development of legislative and regulatory frameworks, and safeguards the integrity of card payments by tackling card fraud, developing industry standards and co-ordinating other industry-wide initiatives. More information about The UK Cards Association is available at www.theukcardsassociation.org.uk.

4 Financial Fraud Action UK is the umbrella 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 (www.financialfraudaction.org.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 and the Cheque & Credit Clearing Company on credit clearing and cheque fraud.

5 The Fraud Control Steering Group is an unincorporated association of financial institutions who participate in retail banking and the payments market in the UK. It is responsible for formulating and implementing policy and ensuring a co-ordinated industry approach to fighting payment, cheque and lending fraud.

6 The Cheque & Credit Clearing Company (C&CCC) is the industry body that manages the cheque clearing system in Great Britain, including the processing of bankers' drafts, building society cheques, postal orders, warrants and government payable orders. Its wide remit also covers the management of the systems for clearing paper bank giro credits, euro-denominated cheques and US Dollar cheques. C&CCC shares information with Financial Fraud Action UK regarding fraudulent activity in the cheque and credit clearing world.

7 The Dedicated Cheque and Plastic Crime Unit (DCPCU) is a squad of police officers and banking fraud investigators who work together to help reduce the UK's card and cheque fraud losses. The Unit is fully sponsored by the banking industry.

Websites to visit for more information:

www.financialfraudaction.org.uk

www.becardsmart.org.uk

www.identitytheft.org.uk

www.chequeandcredit.co.uk

www.banksafeonline.org.uk