ADDRESS
2 Thomas More Square
London
E1W 1YN

WEBSITE
www.financialfraudaction.org.uk

DIRECT LINE
020 3217 8251

EMAIL
press@paymentscouncil.org.uk

PRESS RELEASE

Embargoed: Not for release before 00:01am 27 September 2012

Deception crimes drive small increase in card fraud and online banking fraud losses

- **Card fraud losses as a proportion of the amount we spent on our cards decreases – from 0.066% during January to June 2011 to 0.063% during the first half of this year**
- **Payment fraud losses are only half a per cent of all fraud losses in the UK**
- **Figures suggest fraudsters bypassing security safeguards by duping consumers into handing over their own details – industry redoubles efforts to support vulnerable customers**

New figures released today (27 September 2012) show that basic frauds, such as distraction thefts and people being tricked into giving their cards, PINs and financial passwords to criminals, have contributed to a small overall increase in card fraud and online banking fraud losses. Cheque fraud losses have also increased, but phone banking losses have fallen by a fifth.

According to The UK Cards Association, **total fraud losses on UK cards** totalled £185.0 million between January and June 2012. This is a 9 per cent increase on losses in the first half of last year (£169.8 million), but represents a fall of 39% from the total of £304.2 million in the first half of 2008 when fraud was at its peak. Additionally, card fraud losses as a proportion of the amount we spent on our cards has actually decreased – from 0.066% during January to June 2011 to 0.063% during the first half of this year. With technology such as chip and PIN helping to deter fraud, criminals have turned their attention to more straightforward ways of getting hold of people's cards and PINs. This includes distracting people in shops or at cash machines and then stealing their cards without them noticing, as well as simply tricking them into handing over their cards and PINs on their own doorstep. For example, elderly customers are called by someone claiming to be from their bank and then being told that their debit or credit card needs collecting. From there, they are asked to key in their PIN, following which a courier is sent by the fraudster to collect the card. Four-fifths (80%) of consumers surveyed earlier in 2012 felt anyone could be a potential victim to this fraud, which police warn is on the increase.

As consumer awareness of these scams can help prevent these losses, the industry launched two public awareness campaigns earlier this year[1]. These advised cardholders to follow simple steps to protect their cards and card details, urging them to be on their guard if they receive phone calls or emails out of the blue from someone claiming to be from their bank or the police. A customer checklist of ways in which consumers can protect themselves from these forms of deception is provided following the detailed break-down of fraud figures.

…more

1 – see Notes to Editors

Online banking fraud losses totalled £21.6 million during January to June 2012 – a 28 per cent increase on the 2011 half-year figure. This has been driven by a huge increase in the number of phishing websites set up by criminals as part of a scam to trick customers into visiting these fake websites and disclosing their online banking login details. Losses in this area also reflect the trend in card fraud, with deception scams resulting in increases. Online banking customers are being tricked into divulging their online login details and passwords over the phone to someone they believe is from their bank but is actually a fraudster.

Phone banking fraud losses fell to £6.7 million (a 21 per cent decrease) during January to June 2012. This reduction is partly down to the fact that criminals are focusing their efforts on fraudulently accessing accounts online rather than over the phone.

Cheque fraud losses increased from £16.4 million in the first half of 2011 **to £17.9 million** during the same period in 2012. Although this is a nine per cent increase, the overwhelming majority of this type of fraud is stopped before the cheque is paid. In fact, £241.3 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 put these industry payment fraud losses into perspective. The NFA estimates that fraud in all its guises cost the UK more than £73 billion a year – card and banking fraud only accounts for just over half a 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 legally protected from financial loss.

DCI David Carter, 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:

"This increase is due to organised criminal gangs committing straightforward frauds, and our focus remains on targeting those responsible and bringing them to justice. And given this rise in old fashioned crimes – criminals using distraction techniques and duping people into disclosing their passwords and online banking details - we are urging everyone to be on their guard and work with us to help stop this criminal activity. Your bank or the police will never cold call you or email you and ask you for your full login details, cards or PINs. If anyone does, hang up the phone or delete the email."

Half-yearly plastic card fraud losses on UK-issued cards January to June 2008 to January to June 2012

Card Fraud Type – on UK issued credit and debit cards	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	Jan-June 2012	+/- 11/12
Phone, internet and mail order fraud (Card-not-present fraud)	£163.9m	£134.0m	£118.2m	£109.2m	£115.8m	+6%
Counterfeit (skimmed/cloned) fraud	£88.8m	£46.3m	£28.2m	£18.0m	£20.2m	+13%
Fraud on lost or stolen cards	£26.8m	£25.1m	£21.3m	£25.7m	£28.0m	+9%
Card ID theft	£19.5m	£23.9m	£15.0m	£11.5m	£14.6m	+27%
Mail non-receipt	£5.3m	£3.5m	£3.8m	£5.4m	£6.4m	+18%
TOTAL	**£304.2m**	**£232.8m**	**£186.8m**	**£169.8m**	**£185.0m**	**+9%**
Contained within this total:						
UK retail face-to-face transactions	£47.3m	£34.7m	£33.8m	£22.3m	£26.5m	+19%
UK cash machine fraud	£20.9m	£20.3m	£17.0m	£15.2m	£14.6m	-3%
Domestic/International split of total:						
UK fraud	£181.8m	£165.6m	£135.2m	£130.4m	£138.9m	+6%
Fraud abroad	£122.4m	£67.1m	£51.5m	£39.4m	£46.1m	+17%

...more

Cheque fraud losses January to June 2008 to January to June 2012

	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	Jan-June 2012	+/- 11/12
Cheque fraud	£21.2m	£15.6m	£14.0m	£16.4m	£17.9m	+9%

Half-yearly remote (online and phone) banking fraud losses January to June 2008 to January to June 2012

	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	Jan-June 2012	+/- 11/12
Online banking fraud losses	£25.2m	£39.0m	£24.9m	£16.9m	£21.6m	+28%
Phone banking fraud losses	-	£5.3m	£5.8m	£8.6m	£6.7m	-22%
Remote banking fraud losses	-	**£44.3m**	**£30.7m**	**£25.5m**	**£28.3m**	**+11%**

Online banking fraud: No. of phishing websites	20,682	26,045	31,448	37,198	111,396	+/- +199%

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

The industry is today launching a Call to Action for consumers to shield themselves from becoming victims of fraud by following the following top tips:

** Ensure you are the only person who knows the PIN for your card.*
** Your bank or the police will **never** phone or email you and ask you to disclose the PIN for your card.*
** 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'.*
** Shield the PIN for your card with your free hand when typing it into a keypad in a shop or at a cash machine.*
** Check your bank and card statements for unusual transactions. If you spot any let your bank or card company know as soon as possible.*
** Only shop on secure websites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser.*
** Make sure you have up-to-date anti-virus software installed on your computer.*
** Rip up or preferably shred statements, receipts and documents that contain information relating to your financial affairs when you dispose of them.*
** 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.*

ENDS

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

Notes to editors:

1 **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.

2 **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 (an unincorporated association of financial institutions who participate in retail banking and the payments market in the UK) on non-card fraud and the Cheque & Credit Clearing Company on credit clearing and cheque fraud.

3 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 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.

4 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.

5 The banking industry has launched two public awareness campaigns this year to advise people about the increase in these low-tech frauds:

The ***Devil's in Your Details*** was a video-driven campaign that launched in March 2012 to raise awareness of the importance of protecting personal information as well as educating people on how they can protect themselves, by outlining what they should look out for when it comes to fraud and the methods fraudsters use to target them. This was complemented by a hard-hitting viral Facebook campaign, which took users names and profile pictures and put them into an undercover video report. The campaign can be seen at **www.thedevilsinyourdetails.com**

The ***Hang Up On Fraud*** campaign was launched in May 2012 and raised awareness of a sophisticated type of fraud – where people are telephoned by fraudsters and duped into revealing their PIN and handing over their bank card to a courier. It begins with the 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.

6 A number of banking industry initiatives continue to tackle fraud in all its guises:

- 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 £400 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).

- Banks and card companies use intelligent fraud detection systems, 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.

Websites for more information: www.financialfraudaction.org.uk, www.chequeandcredit.co.uk, www.banksafeonline.org.uk