ADDRESS
2 Thomas More Square
London
E1W 1YN

WEBSITE
www.financialfraudaction.org.uk

DIRECT LINE
020 3217 8251

EMAIL
press@ukcards-ffauk.org.uk

NEWS RELEASE

Embargoed: Not for release before 00:01am 12 March 2013

DECLINE IN FRAUD LOSSES STALLED BY RISE IN DECEPTION CRIMES AIMED AT CONSUMERS

- **Low-tech deception crimes are the new front in the fight against fraud, as figures show 14% rise in fraud losses on debit and credit cards from last year's ten year low**

- **Despite the recent increase, fraud continues to remain low compared to previous peaks: card fraud losses drop 36%; the amount lost to fraud as a proportion of the amount we spent on our cards represents only 7p of losses for every £100.**

- **Total net remote banking fraud losses for 2012 are flat, with telephone banking fraud losses falling by a quarter.**

New figures released today (12 March 2013) show that a return amongst criminals to traditional methods of fraud, such as low-tech deception crimes, has led to increased fraud losses borne by the banking industry. Experts have highlighted the impact of improved security features, such as Chip & PIN and more sophisticated detection tools, which have driven criminals to resort to deceiving consumers into such things as parting with their own cards, PINs and financial passwords. The industry has responded by re-doubling efforts to re-educate and encourage consumers to protect their details, with targeted campaigns being delivered to reach specific groups of customers who are at higher risk of being approached.

Fraud losses on UK cards totalled £388 million in 2012, showing a 14% increase from total fraud losses of £341m in 2011. This increase follows three years of significant decreases (2012 losses of £388m versus 2008 losses of £610m when fraud was at its peak, representing an overall decrease of 36%) with fraud dropping to a ten-year low in 2011. Efforts by the cards industry to enhance the security of payment systems has delivered substantial falls since fraud peaked in 2008.

Interrupting this decline, new fraud intelligence has shown that the 2012 rise was driven by crude scams designed to bypass security systems by duping consumers into handing over their own cards and PINs. This includes distracting people in shops and bars, or shoulder surfing at cash machines and then stealing customers' cards without them noticing, or even tricking them into handing over their card details on their own

doorstep. Another major factor has been UK cards being compromised and used in countries where security levels are lower than in the UK, for example where those countries have not yet moved to Chip and PIN.

Losses on Card-Not-Present transactions (those conducted online and over the telephone) rose by 11% in 2012, but this needs to be seen in the context of the sharp 18% increase in card spending on the internet (reaching £63bn) over the last year.

Despite the overall 2012 increase, the chances of becoming a victim are still low: the amount lost to fraud as a proportion of the amount we spent on our cards represents only 7p of losses for every £100, which is down from 12p per £100 recorded in 2008.

In response, the card payments industry has reiterated its message to consumers that banks and the police will NEVER phone or email customers to ask them to disclose their PIN. Activity has also been undertaken by officers at the industry-sponsored Dedicated Cheque and Plastic Crime Unit (DCPCU) to demonstrate to customers the importance of shielding their PIN at cashpoints. A checklist of ways in which consumers can protect themselves from these forms of deception is provided following the detailed break-down of fraud figures.

Online banking fraud rose 12 per cent to £39.6m from £35.4m in 2011. This increase has been largely driven by fake websites which have tricked consumers into giving away their online banking login details. These 'phishing' emails and sites, which were on the rise for most of 2012, are set up by criminals to trick vulnerable customers into believing they are communicating with their bank or building society. Evidence shows that online banking customers are also being tricked into divulging their login details, passwords and other personal data over the phone to someone they believe is from their bank but is actually a fraudster.

In response, the industry is working with the Serious Organised Crime Agency (SOCA), the Police Central e-crime Unit (PCeU), overseas law enforcement agencies, technology companies and Internet Service Providers (ISPs) to detect and close down phishing websites. Encouragingly, sustained police attention has led to phishing incidents falling significantly during the final quarter of 2012. Alongside this, the introduction of online banking password-generators has had a notable impact in enhancing security.

Telephone banking fraud losses fell to £12.6m in 2012 from £16.7m in 2011 (a decrease of 25%). This reduction reflects the success of procedures used by banks to confirm customers' identity, but has led to criminals focusing their efforts on fraudulently accessing accounts online rather than over the phone.

The effect of these two sets of figures is that the **combined total net remote banking (online and telephone) fraud losses for 2012 are flat.**

Cheque fraud losses rose 2 per cent to £35.1m in 2012 from £34.3m in 2011. The rise can be attributed to fraudsters stealing genuine cheques and altering the payee name or using details from genuine cheques to create counterfeits. This new figure represents a decrease when compared to a peak in 2008, when losses were 16% higher. The overwhelming majority of this type of fraud is stopped before the cheque is paid: in fact, 93% of attempted cheque fraud was spotted and prevented during the clearing process in 2012. Law enforcement has also played a major role, with the industry-sponsored Dedicated Cheque and Plastic Crime Unit (DCPCU) having dismantled what is believed to be one of the UK's biggest counterfeit cheque crime groups, worth in excess of £5 million, last year.

Fraud figures published by the National Fraud Authority (NFA) put these payment fraud losses into perspective. The NFA estimates that fraud in all its guises cost the UK more than £73 billion a year during

2011 – card and banking fraud only **accounts for just over half a per cent** of this figure. Importantly, regulation ensures that the victims of fraud will be protected against any losses. Recent industry data found that **97% of all claims resulted in a full refund of losses** to the customer, a figure which was confirmed by recent research published by Which? magazine which put the figure receiving refunds at 98%.

Detective Inspector David Timmins, from the Dedicated Cheque and Plastic Crime Unit (DCPCU) said:

"This latest set of national figures demonstrates the new frontline in the fight against fraud. As a consequence of more robust security features, criminals are resorting to low-tech deception crimes designed to dupe customers into parting with their cards, PINs and financial passwords. These fraudsters can be highly persuasive, so our message to customers is simple: your bank or the police will never call, visit or email you to request your login details or PIN, or to collect your card. If you receive such a request, it will always be fraud, so protect yourself and call the police".

Annual fraud losses on UK-issued cards 2007-2012

Card Fraud Type on UK-issued credit and debit cards	2007	2008	2009	2010	2011	2012	% +/- 11-12
Telephone, internet and mail order fraud (card-not-present fraud)	£290.5m	£328.4m	£266.4m	£226.9m	£220.9m	£245.8m	+11%
Counterfeit (skimmed/cloned) fraud	£144.3m	£169.8m	£80.9m	£47.6m	£36.1m	£42.1m	+16%
Fraud on lost or stolen cards	£56.2m	£54.1m	£47.7m	£44.4m	£50.1m	£55.2m	+10%
Card ID theft	£34.1m	£47.4m	£38.2m	£38.1m	£22.5m	£32.1m	+42%
Mail non-receipt	£10.2m	£10.2m	£6.9m	£8.4m	£11.3m	£12.8m	+13%
TOTAL	£535.2m	£609.9m	£440.0m	£365.4m	£341.0m	£388.0m	+14%
Contained within this total:							
UK retail face-to-face transactions	£73.0m	£98.5m	£71.8m	£67.4m	£43.2m	£54.5m	+26%
UK cash machine fraud	£35.0m	£45.7m	£36.7m	£33.2m	£29.3m	£28.9m	-1%
domestic/international split of total							
UK fraud	£327.6m	£379.7m	£317.4m	£271.5m	£261m	£286.7m	+10%
Fraud abroad	£207.6m	£230.1m	£122.6m	£93.9m	£80m	£101.3m	+27%

Annual online and telephone banking losses 2007 to 2012

	2007	2008	2009	2010	2011	2012	% +/- 11-12
Online banking fraud losses	£22.6m	£52.5m	£59.7m	£46.7m	£35.4m	£39.6m	+12%
Telephone banking fraud losses	-	-	£12.1m	£12.7m	£16.7m	£12.6m	-25%

Phishing attacks (number)	25,797	43,991	51,161	61,873	111,286	256,641	+131%

Cheque fraud losses 2007 to 2012

	2007	2008	2009	2010	2011	2012	% +/- 11-12
TOTAL	£33.5m	£41.9m	£29.8m	£29.3m	£34.3m	£35.1m	2%

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

The industry is today advising consumers to protect 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.*

** Always be suspicious of unsolicited emails that are supposedly from a reputable organisation, such as your bank or the tax office. Check the URL web address. The login page on your bank's website address should start with "https".*

ENDS

For further information please contact the press office on 020 3217 8436 / 07702 428210 or email press@ukcards-ffauk.org.uk

Notes to editors:

1 **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 (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.

2 **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 coordinating other industry-wide initiatives. More information about The UK Cards Association is available at www.theukcardsassociation.org.uk

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 recent public awareness campaigns to advise people about the increase in these low-tech frauds:

> The ***Devil's in Your Details*** was a video-driven campaign that launched 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**
>
> Another national campaign raised awareness of a rising type of fraud where people are telephoned by criminals 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