ADDRESS
2 Thomas More Square
London
E1W 1YN

WEBSITE
www.financialfraudaction.org.uk

DIRECT LINE
020 3217 8436

EMAIL
press@ukcards-ffauk.org.uk

NEWS RELEASE

SCAMS AND COMPUTER ATTACKS CONTRIBUTE TO INCREASE IN FRAUD, AS TOTAL CARD SPENDING RISES

- **Card fraud rises in 2013, but still represents only 7.4p for every £100 spent.**
- **Consumers and online businesses urged to install security software to protect themselves from 'malware' viruses.**
- **Deception crimes – including 'vishing' – continue to be a threat.**
- **Cheque fraud and telephone banking fraud fall by 22% and 8% respectively, with modest 3% rise in online banking fraud.**

New figures released today [14 March 2014] by Financial Fraud Action UK (FFA UK) show that levels of card and online banking fraud rose during 2013. Improved fraud detection and prevention systems used by banks and established internet retailers continue to have a positive impact, but intelligence suggests that criminals are now targeting individual consumers and small businesses – driving the recent reported losses. While consumers are warned to be vigilant, they continue to enjoy strong legal protections against bearing any personal losses – meaning online shopping remains safe and secure.

Fraud losses on UK cards totalled £450.4 million in 2013, a 16 per cent rise on the total in 2012 of £388.3 million. This figure is still down 26 per cent since fraud was at its peak in 2008. At the same time, total spending on all debit and credit cards reached £532 billion in 2013, a rise of 6.1 per cent on 2012, with 10.9 billion transactions made in the year[1].

Overall, card fraud losses as a proportion of the value of purchases on our cards has increased only slightly – from 7.1p for every £100 spent in 2012 to 7.4p in 2013 (in 2008 it was 12.4p for every £100). The total number of all transactions rose by over half a billion between 2012 and 2013.

Losses on remote card purchases (those made online, over the telephone or by mail order) increased by 22 per cent to £301.1 million in 2013, from £246.0 million in 2012.

1 – see Notes to Editors

The UK is Europe's leading online shopping economy with spending by British consumers online growing by 16 per cent in 2013 to reach £91 billion[2]. Card payments are the main driver of this growth as they provide the most effective way to pay online. Debit and credit cards also offer consumers protection against fraud.

Online fraud against UK retailers totalled an estimated £105.5 million in 2013, a rise of 4 per cent on the previous year. However, there has been a substantial increase in fraud against online retailers based overseas, rising 48 per cent to an estimated £57.8 million.

Enhanced card security features, such as Chip & PIN, as well as advanced real-time fraud screening techniques employed by banks and established internet retailers, have forced criminals to change tactics. As well as tricking customers into handing over personal and financial details (including cards and PINs), for example over the telephone while posing as officers from the bank or the police, fraudsters are also increasingly using digital attacks, such as malware and data hacks, to compromise card details.

Malware is malicious software which is unknowingly downloaded onto a computer and which then enables fraudsters to steal personal or financial information or perform unauthorised actions on the device. It is believed criminals are using these stolen details to commit fraud by targeting those online retailers which have not yet adopted security measures put in place by more established firms.

In order to help tackle this trend, experts and the police are urging consumers and online businesses to install security software, often freely available from a customer's own bank. To prevent stolen card details being used to make purchases online, retailers are being advised to take steps to improve their security, including use of the online protection (including American Express' 'Safe Key', 'Verified by Visa' and MasterCard's 'SecureCode') and by following the prevention tips listed below.

Meanwhile, a major national campaign '*Be Cyber Streetwise*' has been launched by the Government, supported by FFA UK and offers further advice that consumers and small businesses can adopt to protect themselves while shopping or banking online.[3]

The card fraud figures are also a reminder to consumers to be vigilant against scams. **Losses due to fraud on lost or stolen cards increased by 7 per cent to £58.9 million** from £55.2 million in 2012, with distraction thefts in shops and bars and shoulder surfing at ATMs highlighted. Meanwhile, 'vishing' over the telephone, with fraudsters tricking consumers into parting with personal or financial information, has been identified as a driver for the **14 per cent rise in card ID theft to £36.7m** from £32.2m. In response, the industry is highlighting to consumers the 'golden rule' that the bank and the police will NEVER phone or email customers asking for their PIN or full online banking codes, or visit their home to collect a bank card.

Online banking fraud has increased by 3 per cent to £40.9 million from £39.6 million in 2012. Intelligence shows this increase has also been driven by the rise in 'vishing' and malware. Fraudsters are increasingly targeting business customers rather than personal accounts due to the prospect of a potentially higher return.

Telephone banking fraud has fallen 8 per cent to £11.6 million from £12.6 million in 2012**.** This fall has been as a result of tighter processes by banks which are designed to confirm customers' identity.

Cheque fraud losses fell 22 per cent to £27.5 million from £35.1 million in 2012. Improved fraud detection methods used across the industry, including the digital analysis of cheques, has led to the considerable decrease.

Detective Chief Inspector Perry Stokes, Head of the Dedicated Cheque and Plastic Crime Unit, said:

"Whether in the real world or online, these latest fraud figures show just how important it is for consumers and businesses to know how to protect themselves against fraud. Always make sure you have the latest security software installed on your computer, so you can safely shop and bank online.

"Fraudsters can be extremely persuasive – do not be fooled. Your bank or the police will never call, visit or email you to request your PIN, collect your bank card, or ask you to transfer money to another account. Anyone attempting to do so is a fraudster."

Annual fraud losses on UK-issued cards 2007 to 2013

Card Fraud Type on UK-issued credit and debit cards	2007	2008	2009	2010	2011	2012	2013	% +/- 12-13
Telephone, internet and mail order fraud (remote purchase fraud)	£290.5m	£328.4m	£266.4m	£226.9m	£220.9m	£246.0m	£301.1m	+22%
Counterfeit (skimmed/cloned) fraud	£144.3m	£169.8m	£80.9m	£47.6m	£36.1m	£42.1m	£43.4m	+3%
Fraud on lost or stolen cards	£56.2m	£54.1m	£47.7m	£44.4m	£50.1m	£55.2m	£58.9m	+7%
Card ID theft	£34.1m	£47.4m	£38.2m	£38.1m	£22.5m	£32.2m	£36.7m	+14%
Mail non-receipt	£10.2m	£10.2m	£6.9m	£8.4m	£11.3m	£12.8m	£10.4m	-19%
TOTAL	£535.2m	£609.9m	£440.0m	£365.4m	£341.0m	£388.3m	£450.4m	+16%
Contained within this total:								
UK retail face-to-face transactions	£73.0m	£98.5m	£71.8m	£67.4m	£43.2m	£54.6m	£60.8m	+11%
UK cash machine fraud	£35.0m	£45.7m	£36.7m	£33.2m	£29.3m	£28.9m	£31.9m	+10%
domestic/international split of total								
UK fraud	£327.6m	£379.7m	£317.4m	£271.5m	£261m	£286.7m	£328.4m	+14%
Fraud abroad	£207.6m	£230.1m	£122.6m	£93.9m	£80m	£101.3m	£122m	+20%

Annual online and telephone banking losses 2007 to 2013

	2007	2008	2009	2010	2011	2012	2013	% +/- 12-13
Online banking fraud losses	£22.6m	£52.5m	£59.7m	£46.7m	£35.4m	£39.6m	£40.9m	+3%
Telephone banking fraud losses	-	-	£12.1m	£12.7m	£16.7m	£12.6m	£11.6m	-8%

Annual cheque fraud losses 2007 to 2013

	2007	2008	2009	2010	2011	2012	2013	% +/- 12-13
TOTAL	£33.5m	£41.9m	£29.8m	£29.3m	£34.3m	£35.1m	£27.5m	-22%

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

Advice to consumers on how to take steps to avoid becoming a fraud victim:

- Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software: check your bank's website for details.
- Only shop on secure websites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser.
- Always be suspicious of unsolicited emails that are supposedly from a reputable organisation, such as your bank or the tax office and do not click on any links in the email.
- Make sure you are the only person who knows the PIN for your card.
- Be aware: Your bank or the police will never phone, email or visit you to ask you for card PIN or to pick up your card. Never hand your card over to anyone who comes to 'collect it'.
- Shield the PIN with your free hand whenever you type 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.
- Rip up or preferably shred statements, receipts and documents that contain information relating to your financial affairs when you dispose of them. Some banks offer paperless statements.
- 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.

Advice to businesses on how to take steps to avoid becoming a victim of remote purchase fraud:

- Ask your bank or card processor about the online protection offered by card schemes, such as Verified by Visa, SecureCode by MasterCard and American Express' 'Safe Key', which help make transactions over the internet safer from the threat of fraud.
- Know your customer: assess a customer's profile, order and delivery details before accepting a transaction.
- Be wary of high value or unusual orders from customers you do not know, particularly if the product is easily resalable.
- Use the banking industry's Address Verification Service, which compares the delivery address provided for the order with the billing address details for the payment card held by the card issuer.
- Maintain a record of fraudulent accounts and transactions to prevent further breaches – fraudsters will continue to attack businesses until the window of opportunity is closed.

ENDS

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

Notes to editors:

1. UK Cards Association Card Expenditure Statistics December 2013 (http://www.theukcardsassociation.org.uk/2013-facts-figures/index.asp).

2. Figures on spending on online purchases at British online retailers from IMRG: http://www.imrg.org/index.php?catalog=539

3. HM Government's new Cyber Street resource, providing interactive resources, can be found at: www.cyberstreetwise.com

4. **Financial Fraud Action UK** (FFA 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.

5. **The UK Cards Association** is the trade body for the card payments industry in the UK, representing financial institutions which act as card issuers and acquirers. Members of the Association account for the vast majority of debit and credit cards issued in the UK - issuing in excess of 56 million credit cards and 88 million debit cards - and cover the whole of the payment card acquiring market.

More information about The UK Cards Association is available at www.theukcardsassociation.org.uk.

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 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.

More information about The Cheque & Credit Clearing Company is available at www.chequeandcredit.co.uk

7. **The Dedicated Cheque and Plastic Crime Unit** (DCPCU) is a unique pro-active police unit, with a national remit, formed as a partnership between Financial Fraud Action UK, the City of London Police and the Metropolitan Police together with the Home Office. It is fully sponsored by the cards and banking industries, with an on-going brief to investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for card, cheque and payment fraud crimes. It is headed up by a Detective Chief Inspector and comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators and support staff.

8. 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 (remote purchase 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 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 and www.chequeandcredit.co.uk.

Follow us on Twitter: @FFAUK
Visit us on Facebook