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

CUSTOMERS URGED TO BE VIGILANT AS FRAUDSTERS INCREASE SCAM ATTACKS

- **Card fraud rises, but as a proportion of spending remains flat at 7.4p for every £100 spent during first half of 2014**

- **Rise in remote banking fraud losses as criminals target businesses and consumers through telephone 'Vishing' and computer viruses**

- **Banks highlight warning signs of scams, and support calls made by City of London Police Commissioner for national awareness campaign**

New figures released today [12 September 2014] by Financial Fraud Action UK (FFA UK) show that card and remote banking fraud increased during the first six months of 2014. The intelligence behind the figures reinforces recent trends, which have seen the growth of deception crimes seeking to persuade consumers to part with their personal and financial information, as well as criminals' use of computer viruses. As a result, customers are being warned to be vigilant and be aware of the key warning signs of scams.

Fraud losses on UK cards totalled £247.6 million between January and June 2014, an increase of 15 per cent from £216.1 million during the same period in 2013. Fraud as a proportion of card purchases has remained flat at **7.4p for every £100 spent**, the same proportion as the industry reported at the end of 2013.

Losses on remote banking fraud rose to £35.9 million, up 59 per cent from £22.6 million in 2013. Within this total, online banking fraud losses rose to £29.3 million, up 71 per cent from £17.1 million in 2013. Telephone banking fraud rose to £6.6 million, up 20 per cent from £5.5 million. Intelligence suggests criminals are targeting business accounts which typically allow higher value fraudulent transactions.

Losses due to remote card purchases (those made online, over the telephone or by mail order) rose to £174.5 million in the first six months of 2014, up 23 per cent from £142.0

million in the same period in 2013. Within this total, the e-commerce fraud loss is estimated to be £110.0 million, up 23 per cent from an estimated £89.5 million in the first half of 2013.

While significant, this rise needs to be viewed in context of the increase in internet shopping by British consumers, with spending up from an estimated £40.5 billion in the first half of 2013 to an estimated £47 billion in the same period in 2014, according to IMRG [1]. Card payments are the main driver of online spending growth as they provide the most effective way to pay online.

A key driver for the rise in fraud losses has been the growth of deception crimes aimed at individuals and businesses. A combination of Chip & PIN and advanced fraud screening detection processes used by the banks drove a long-term decline in card fraud up to 2012. This is illustrated by the 72 per cent decline in high street fraud losses between 2004 and 2013. In response, fraudsters are increasingly concentrating their efforts on obtaining personal and financial details from individual customers rather than attacking the security systems used by the banks.

An increasing problem has been criminals telephoning people at home while posing as the bank, police or representatives of other trusted organisations, such as Government departments. These cold-calls typically involve the fraudster tricking their victim into revealing personal or financial information, such as their 4 digit PIN or online banking details; transferring money to another account; or accepting a courier into their home to pick up their card.

Once details have been compromised, they are then used to commit fraud through both remote (telephone or online) banking channels and through shopping online. Commonly, fraudsters target retailers who have not introduced adequate internet shopping protections.

Research conducted by ICM for FFA UK showed that a quarter (25 per cent) of customers do not take steps to challenge the identity of a cold-caller, with this figure rising to 34 per cent of 18-24 year-olds [2].

To stop these scams, police and fraud experts are highlighting the key warning signs:

Your bank will <u>never</u>:

- Call you and ask for your 4 digit PIN or your FULL online or telephone banking security codes over the phone.
- Ask you to withdraw money to hand over to them, or to transfer money to another account, even if they say the account is in your name.
- Come to your home to collect your cash, payment card or cheque book.
- Ask you to purchase goods using your card and then hand them over for safe keeping.

Intelligence also shows criminals are using computer viruses to steal personal and financial information, which is then used to commit fraud. FFA UK strongly endorses the call to action by the National Crime Agency last month for consumers to download and update their security software. Free software is often available for customers to download from their banks' website.

Distraction thefts in shops and at ATMs have been identified as a driver of **fraud on lost or stolen cards, which has increased by 3 per cent to £29.2 million** from £28.2 million in the

first half of 2013. Meanwhile, **mail non-receipt fraud has increased 10 per cent to £5.0 million**, up from £4.6 million, with fraudsters targeting multiple occupancy residences to intercept cards and personal details from post boxes.

Counterfeit card fraud rose by 4 per cent in the first 6 months of 2014 to £24.2 million, up from £23.3 million in 2013. The key driver for this modest rise is that stolen card details in the UK are being used to create counterfeit cards for use overseas in countries which have not yet implemented Chip & PIN.

Fraud on contactless cards continues to be negligible at £51,000 over the first six months of the year, which is just 0.007 per cent of contactless card spending.

Cheque fraud losses fell 34 per cent to £10.5 million in the first half of 2014, from £15.8 million in January to June 2013. The continued success of improved fraudulent cheque detection methods and enhanced prevention controls is the driver for this long-term decline.

The industry is tackling fraud through enforcement, information sharing, technological advances and awareness campaigns. The industry fully sponsors a specialist police unit, the Dedicated Cheque and Plastic Crime Unit (DCPCU), which identifies and targets the organised criminal gangs responsible for payment fraud. Since its inception in 2002, the DCPCU has achieved an estimated £800,000 a week in savings from reduced fraud. Through FFA UK, the card and retail banking industry securely shares intelligence on emerging threats and identifies patterns in fraud which protect consumers and strengthen the industry's defences. Banks use a range of increasingly sophisticated fraud screening detection tools to prevent fraudulent transactions. FFA UK will shortly be launching a 'vishing' awareness initiative aimed at increasing customer vigilance of the scams.

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

"Be very suspicious of phone calls, texts or emails which come out of the blue asking for personal or financial details, regardless of who they claim to represent.

"Be aware of the warning signs: your bank will never ask you for your 4 digit PIN, to transfer or withdraw money, or to give your card to a courier. We are asking members of the public to pass this information on to any family and friends who may be unaware, and echo calls made last week by the Commissioner of City of London Police for a national awareness-raising campaign led by Government."

Full fraud figures overleaf

Half year fraud losses on UK-issued cards 2008 to 2014

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	Jan-June 2013	Jan-June 2014	% +/- 13-14
Telephone, internet and mail order fraud (remote purchase fraud)	£163.9m	£134.0m	£118.2m	£109.2m	£115.8m	£142.0mn	£174.5m	23%
Counterfeit (skimmed/cloned) fraud	£88.8m	£46.3m	£28.2m	£18.0m	£20.2m	£23.3m	£24.1m	4%
Fraud on lost or stolen cards	£26.8m	£25.1m	£21.3m	£25.7m	£28.0m	£28.2m	£29.2m	3%
Card ID theft	£19.5m	£23.9m	£15.0m	£11.5m	£14.6m	£18.1m	£14.7m	-19%
Mail non-receipt	£5.3m	£3.5m	£3.8m	£5.4m	£6.4m	£4.6m	£5.0m	10%
TOTAL	**£304.2m**	**£232.8m**	**£186.8m**	**£169.8m**	**£185.0m**	**£216.1m**	**£247.6m**	**15%**
Contained within this total:								
UK retail face-to-face transactions	£47.3m	£34.7m	£33.8m	£22.3m	£26.5m	£27.2m	£35.9m	32%
UK cash machine fraud	£20.9m	£20.3m	£17.0m	£15.2m	£14.6m	£16.2m	£14.3m	-12%
domestic/international								
UK fraud	£181.8m	£165.6m	£135.2m	£130.4m	£138.9m	£155.9m	£175.2m	12%
Fraud abroad	£122.4m	£67.1m	£51.5m	£39.4m	£46.1m	£60.2m	£72.4m	20%

Half year online and telephone banking losses 2008 to 2014

	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	Jan-June 2012	Jan-June 2013	Jan-June 2014	% +/- 13-14
Online banking fraud losses	£25.2m	£39.0m	£24.9m	£16.9m	£21.6m	£17.1m	£29.3m	71%
Telephone banking fraud losses	-	£5.3m	£5.8m	£8.6m	£6.7m	£5.5m	£6.6m	20%
Remote banking fraud losses	-	£44.3m	£30.7m	£25.5m	£28.3m	£22.6m	£35.9	59%

Half year cheque fraud losses 2008 to 2014

	Jan-June 2008	Jan-June 2009	Jan-June 2010	Jan-June 2011	Jan-June 2012	Jan-June 2013	Jan-June 2014	% +/- 13-14
Cheque fraud	£21.2m	£15.6m	£14.0m	£16.4m	£17.9m	£15.8m	£10.5m	-34%

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

Consumers have strong legal protections against bearing any personal losses when debit and credit cards are misused by fraudsters.

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

- 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, ask you to transfer money to another account, or to withdraw money over the counter. 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.
- 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.
- 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. Figures on spending on online purchases at British online retailers from IMRG: http://www.imrg.org/index.php?catalog=1067

2. Research was carried out by ICM from 8 August to 10 August with 2005 people surveyed.

3. An improvement to the methodology used to estimate the e-commerce element of remote purchase fraud was identified in early 2014 and has been adopted in this release. 2013 figures have also been adjusted.

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 55 million credit cards and 95 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 is helping to prevent criminals from copying or skimming the magnetic stripe details from genuine cards.

As well as introducing additional security measures such as two-factor authentication and free security software for customers, the banking industry works with a number of partners, including the National Crime Agency, the Metropolitan Police Cyber Crime Unit (MPCCU), overseas law enforcement agencies, technology companies, anti-virus firms, telecommunications industry and Internet Service Providers to prevent remote banking fraud.

All banks use sophisticated security systems to protect their customers' accounts. These systems are constantly upgraded to maintain their effectiveness. Collectively, the banking industry shares information and intelligence with law enforcement and the telecommunications industry to identify fraudulent activity and those seeking to undertake it, and to maintain the security of telephone-based services.

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

Follow us on Twitter: @FFAUK
Visit us on Facebook