Financial Fraud Action UK
Working together to prevent fraud

**ADDRESS**
2 Thomas More Square
London E1W 1YN
**TELEPHONE**
020 3217 8200
**WEBSITE**
www.financialfraudactionuk.org.uk
**DIRECT LINE**
020 3217 8436
**EMAIL**
press@ukcards-ffauk.org.uk

**28th August 2013**

PRESS RELEASE EMBARGOED UNTIL 00:01 28/08/2013

# QUARTER OF BRITS AT RISK OF 'VISHING'

## Fraudsters pose as legitimate organisations to steal personal and financial information over the phone

Financial Fraud Action UK (FFA UK) has released new fraud intelligence highlighting the growth of a particular type of phone scam in which fraudsters are targeting individuals to deceive them into revealing personal and financial information - or make payments into the fraudster's account.

FFA UK has seen an overall increase of £36m across remote banking and remote purchase (telephone and online), account takeover, and application fraud in the last financial year[1]. Early estimates indicate that at least £7m worth may be attributed to the scam, called 'Vishing'[2].

Findings suggest that one in twenty-five adults in the UK may have been a victim of 'Vishing'[3], with 43% of those victims aged over 50 years old.

Almost a quarter of people in the UK (23 per cent) have received a cold call requesting personal or financial information, potentially putting them at risk of becoming a victim of Vishing. Four in ten people (39 per cent) admitted they found it challenging to tell the difference between a genuine and fraudulent call.

Almost a third (30 per cent) of the UK population received at least 10 cold calls per month, with 41 per cent suspecting that a call was fraudulent or suspicious. However, when it came to those aged over 50, this group were shown to be particularly at risk, with almost half (47 per cent) having received a fraudulent or suspicious cold call.

Vishing involves a fraudster making a phone call to a potential victim, posing as someone from a bank or building society fraud investigation team, the police or another legitimate organisation such as a telephone or internet provider. They attempt to obtain financial information which often includes credit/debit card details (including PIN), bank account details and personal information such as full name, date of birth or address. This information is then used by the fraudster to gain access to their victim's finances.

Fraudsters can also deceive the victim into transferring money themselves from their own bank account to one which is accessible to the fraudster. A variation on this scam involves the victim being persuaded to withdraw money from a branch or ATM to pay the fraudster.

DCI Dave Carter, Head of the Dedicated Cheque and Plastic Crime Unit (DCPCU), a pro-active police unit that is fully sponsored by the cards and banking industries
[Available for interview] said:

“Fraudsters can use personal information gleaned from Vishing in a number of ways including to access a victim’s bank account, make fraudulent purchases and commit identity theft.

“Always be wary of cold callers who suggest you hang up the phone and call them back. Fraudsters will keep your phone line open by not putting down the receiver at their end. Remember that it takes two people to terminate a call so try and use a different phone line if you are asked to ring back. If you think you’ve already been a victim of this scam, contact your bank or card company immediately.”

**Advice to consumers on how to take steps to avoid this type of scam:**

**Be wary of:**

- unsolicited approaches by phone.
- cold callers who suggest you hang up the phone and call them back. Fraudsters can keep your phone line open by not putting down the receiver at their end.

**Never disclose your**

- 4 digit card PIN to anyone, including the bank or police.
- FULL password or online banking codes[4.]
- Personal details unless you are sure who you are talking to.

**Your bank or the police will never**

- ask for your 4 digit card PIN.
- ask you to withdraw money to hand over to them or transfer money to another account, even if they say it 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.

**Remember**

- It takes two people to terminate a call, you can use a different phone line to return the call if you can.
- If you are unsure about providing the information your caller has requested, visit your bank’s website to check their policy on what information they will and won’t ask for.
- If you are suspicious or feel vulnerable, don’t be afraid to terminate the call, and say no to requests for information.
- Criminals may already have basic information about you in their possession (e.g. name, address, account details), so do not assume a caller is genuine because they have these details or because they claim to represent a legitimate organisation.

- Ends –

For further information, spokesperson request or case study details please contact the Financial Fraud Action UK press office on 020 3217 8436 or email press@ukcards-ffauk.org.uk

**Notes to editors**

1. Financial Fraud Action UK's member recorded figures between the periods April 2011 to March 2012 and April 2012 to March 2013.

2. Financial Fraud Action UK's member intelligence from the period April 2012 to March 2013.

3. Research was carried out by ICM from 31 July to 1 August with 2002 respondents surveyed.

4. Different banks use different systems or authentication devices to prove that you are the genuine customer. Some may issue you with a key-fob device that produces a one-time passcode. Others may provide you with a pocket-sized card reading device that you insert your debit card into, which also produces a one-time passcode. This passcode can then be used as one of the security steps needed to login to your online banking website or to authorise a payment.

**About Financial Fraud Action UK (FFA 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.

**About Dedicated Cheque and Plastic Crime Unit (DCPCU)**
The 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. The Unit has been responsible for estimated savings of over £433 million since its launch in 2002.