



Financial Fraud Action UK
Working together to prevent fraud

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

NEW FIGURES SHOW STEEP RISE IN TELEPHONE SCAMS

Embargoed until 00.01 Tuesday 2 December 2014

- **TREBLING OF LOSSES OWED TO ‘VISHING’ SCAMS**
- **17% INCREASE IN NUMBER OF CONSUMERS RECEIVING SUSPICIOUS CALLS**
- **‘JOINT DECLARATION’ OF THE UK BANKS LAUNCHED**

New figures published today (Tuesday 2 December) by Financial Fraud Action UK (FFA UK) show a significant rise in the number of consumers who have been targeted by phone scammers over the last year.

The research, carried out on behalf of FFA UK by ICM, suggests that **58 per cent of people have received suspect calls, a steep rise from 41 per cent of respondents** in a similar study carried out last summer.

The increase in scam calls is reflected in new figures, also published today, which show a threefold rise in the amount of money lost to phone scammers. Over the last year, at least **£23.9m of losses can be attributed to Vishing – up from £7m** in the previous year.

In response, a rare **‘Joint Declaration of the UK Banks’ supported by Police** [attached], launched today, has brought together banks, building societies and card companies, as well as Chief Police Officers, to clarify the warning signs of a phone scam. This will be supported by a national advertising campaign to convey these messages to households across the UK.

These 'cold call' scams typically involve fraudsters deceiving victims into believing they are speaking to a police officer, a member of bank staff, or a representative of another trusted organisation, such as a computer company. Typically, the criminal will convince an individual that they have been a victim of fraud, and will ask for personal and financial information in order to gain access to their account. This can include card details, four digit PINs and passwords. Other variations of the scam involve the fraudster persuading their victim to transfer money to other accounts, hand over bank cards directly to a courier or withdraw money from a branch.

Despite the growing threat to the public, results from the ICM research found that a **quarter of people (25 per cent)** make no effort to challenge the identity of callers asking for financial information. Meanwhile, **36 per cent of people** said they found it difficult to tell the difference between genuine requests for information on the phone and fraudulent ones.

Worryingly, a sizeable minority said they would comply with fraudulent directions from the criminal, believing these to be genuine requests from their bank. A total of **10 per cent of respondents** said they would either give cash to a 'courier', hand over their card, or move money into another account if requested to do so by a criminal purporting to be from their bank.

In no circumstances, would the bank or police ask customers to take such actions, and such requests will only come from a fraudster. Indicatively, these figures suggest **4.9 million bank customers nationwide would fall into the trap.**

In response, the 'Joint Declaration of the UK Banks' supported by Police, has been issued to reinforce in people's minds the requests the bank or police will NEVER make.

Almost half (41 per cent of respondents) were unaware of the fraudsters' trick of encouraging their victim to call the bank to verify their identity, only to stay on the line, which can remain open for up to two minutes. When the victim picks up the phone to make what they assume is a new call, the criminal's accomplice tricks them into thinking they are now connected to the bank.

DCI Perry Stokes, Head of the Dedicated Cheque and Plastic Crime Unit (DCPCU) – a specialist policing unit funded by the banking industry and a signatory to the Joint Declaration – said:

“Always be on your guard if you receive a cold call and are asked for personal or financial information, or to hand over your card or cash to someone. The bank or the police will never tell

you to take such actions, so if you're asked it can only be a criminal attack. Wait five minutes and call your bank, preferably from a different telephone, if you have even the slightest doubt".

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.

Your bank or the police will never:

- Phone you to ask for your 4 digit card PIN or your online banking password, even by tapping them into the telephone keypad.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name.
- Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.
- Ask you to purchase goods using your card and then hand them over for safe- keeping.

Never disclose your:

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

Remember

- It takes **two** people to terminate a call.
 - If you feel something is suspicious or feel vulnerable, hang up, wait five minutes to clear the line, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud.
 - If you don't have another telephone to use, call someone you know first to make sure the telephone line is free.
-

- Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller.
- 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.

DCPCU officers are also working in local communities to educate the general public on how to beat the fraudsters as part of their *Hang Up on Fraud* initiative. Beginning in Glasgow, the DCPCU are attending roadshows and conferences to spread the message that cold callers are not always who they say are.

-Ends-

For further information please contact The Financial Fraud Action UK (FFA 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 cover the period of the last tax year.
2. Research was carried out by ICM in August 2014 with 2005 people surveyed.
3. **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.
4. 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 Service together with the Home Office. It is fully sponsored by the cards and payments 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. Since its inception in 2002, the DCPCU has achieved an estimated £470m in savings from reduced fraud activity.