



Financial Fraud Action UK  
Working together to prevent fraud



## CARD FRAUD TELEPHONE CRIME

Financial Fraud Action UK is advising customers to be aware of a growing type of fraud that involves people being telephoned by fraudsters and duped into handing over their debit or credit card, and revealing their PIN.

### HOW DOES IT HAPPEN?

A fraudster rings you, claiming to be from your bank, saying their systems have spotted a fraudulent payment on your card or that your card is due to expire and needs replacing.

You may be asked to ring back using the phone number on the back of your card - which further convinces you the call is genuine. However, the criminal keeps the line open at their end so, when you make the call, you are unknowingly connected straight back to the fraudster.

Then, by seeming to offer assistance, the fraudster tries to gain your trust. In most cases you are asked to 'cancel' your existing card or 'activate' or 'authorise' a replacement card by keying your PIN into your phone's handset.

The fraudster then poses as a bank representative to pick up your card from your home, sometimes giving you 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 into an envelope.

Once they have your card and PIN the fraudster uses them to spend your money.

A variation of the crime involves the fraudster ringing a prospective victim and claiming to be from the police - again with the aim of going to the victim's home to collect the card and PIN.

### WHAT CAN I DO TO AVOID BEING A VICTIM?

*Remember this advice:*

Your bank or the police will **NEVER** ring you and tell you that they are coming to your home to pick up your card, so never hand it over to anyone who comes to collect it.

Your bank will **NEVER** ask you to authorise anything by entering your PIN into the telephone.

**NEVER** share your PIN with anyone - the only times you should use your PIN is at a cash machine or when you use a shop's chip and PIN machine.

### WHAT SHOULD I DO IF I THINK I MAY HAVE BEEN A VICTIM?

Call your bank or card company immediately on an advertised number. Before dialling, make sure you can hear the dial tone.