

**Frequently Asked Questions about Fraud**

**Q - I think I have been a victim of fraud what should I do**

A - If you think there has been fraud on your card or bank account – or if you suspect anyone has attempted to compromise your financial details – report it immediately to your bank or financial services provider and then contact Action Fraud on 0300 123 2040 or at [www.actionfraud.police.uk](http://www.actionfraud.police.uk/).

**Q – Who are Action Fraud?**

A - Action Fraud is the UK’s national reporting centre for fraud and cybercrime, and takes crime and information reports on behalf of the police and gives advice and fraud prevention guidance.

Action Fraud does not have investigation powers, however, the reports taken by Action Fraud are sent to the National Fraud Intelligence Bureau (NFIB) which is run by the City of London Police, the national lead force for fraud.

The NFIB collates and analyses intelligence on fraud, identifying viable lines of enquiry and developing packages for submitting to a police force for investigation.

**Q - What happens to my report once has it been made to Action Fraud?**

A - After a report has been made to Action Fraud, it will be sent for assessment by the National Fraud Intelligence Bureau (NFIB). The NFIB’s systems assess reports of fraud and cybercrime from across the UK, helping to build a national picture of where fraud and cybercrime is taking place and how. Experts review the data from these reports to decide whether there is enough information to send to a police force for investigation.

**Q - My bank has telephoned me and said there is a problem with my account?**

A - The key thing is to take time to think before you act if you’re asked for your personal or financial details, or to transfer money. Put the telephone down, then contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card. There are also some other simple steps you can take to protect yourself from financial fraud, like having up-to-date software and only shopping on secure websites.

**Q – I have received an email from HMRC stating that I am due a refund**

A – HMRC do not contact customers by email and tell them they are due a refund. The email may look genuine and even contain the correct HMRC telephone number. Do not click any links as this will give your personal information to fraudsters. Delete the email.

**Q – I have received an email from HMRC, The Police, The courts stating that I owe money and must pay by I-Tunes Vouchers**

A – You will not be contacted by any of these organisations and told that you need to pay a fine by I Tunes vouchers. This is a scam. Delete the email and do not worry about it.

**Q – I have been in a relationship with someone on line for a few months now. They work abroad and need my financial assistance, what should I do?**

A – This is a Fraud. The relationship may appear genuine but criminals forge relationships with people to make a financial gain for themselves. Follow this link to get more information on romance fraud and some tips on how to date safely online Get safe online - <https://www.getsafeonline.org/>

**Q – Someone wants to use my account to move money from their account to someone else’s bank account**

A – Be very careful about entering into this sort of behaviour as you may be laundering money for criminals which could see you jailed for up to 14 years

**Q - Where can I go to get more advice on how to protect myself against Fraudsters?**

A - Friends Against Scams Training -<https://www.friendsagainstscams.org.uk/training/friends-elearning>.

Little Book of Big Scams (comprehensive guides to preventing fraud) - <https://www.humberside-pcc.gov.uk/Document-Library/Humberside-Police-LBOBS-Online.pdf>

Take Five Financial Authority Campaign Page to tackle Scams - <https://takefive-stopfraud.org.uk/>

**Q – I have been the victim of fraud am I going to get my money back?**

Bank customers tricked into transferring cash to fraudsters now have more protection and are more likely to get a refund, after most major banks signed up to a new voluntary code.

The voluntary code of practice for authorised push payment (APP) scams states that victims should be reimbursed unless they ignored their bank's warnings about the scam or were "grossly negligent" in transferring the money. APP scams occur when someone transfers money from their own bank account to one belonging to a criminal. The lost money is then transferred to numerous other accounts, often abroad

**Q – Someone has knocked on my door and told me that I need work doing to my property?**

It is always advisable to get at least two quotes if you need building work doing. There are a number of websites that you can use to find a registered and approved tradesman.

