Dealing with fraud

Fact sheet no. 54 Dealing with fraud

October 2018

Use this fact sheet to:

- understand about fraud;
- find out how you can help protect yourself from fraud; and
- learn what to do if you become a victim of fraud.

In partnership:

with Action Fraud

We would like to thank Action Fraud for their help with the writing of this fact sheet.

What is fraud?

Fraud occurs when someone tricks you so that they can benefit financially or in another way. These people are commonly known as fraudsters. There are lots of different types of fraud (also known as 'scams') and some can appear quite realistic.

It is important to be aware of the possible types of fraud so that you can spot them and try to protect yourself in the future. Fraud can happen by phone, text, email, website or face to face. Crime, including fraud, carried out using the internet, computers and laptops is known as cyber crime. It is important to protect yourself in the 'real world' and 'online'. See the section **Preventing fraud** for more information.

Action Fraud, the UK's national reporting centre for fraud, has an alphabetical list of different types of fraud. This fact sheet also includes some examples.

Identity theft

Identity theft happens when fraudsters get access to your personal details, such as your name, address and date of birth. Your personal details are valuable to fraudsters because they can use them to try and take out credit, such as a bank loan, or to buy goods in your name. Identity theft can lead to identity fraud. See the section headed **Identity fraud** for more details.

There are several way that fraudsters try to get your personal details. They could look at information you have placed on social newtwork sites, such as Twitter or Facebook. They could look through rubbish you have thrown away for old bank statements and utility bills. Some fraudsters will try to trick you into giving them your personal details by sending you a 'phishing' email. See the section headed **Phishing emails** for more details.

Phishing emails

Phishing emails are fake emails that look as if they have been sent from a trusted organisation, such as your bank, when they have not. They may say that you need to confirm your security details and ask you to click on a link and type in your details. Some of these fake emails also contain harmful software (also known as 'malware') that tries to get passwords and personal information from your computer. This is a kind of identity theft.

Identity fraud

This is when your personal details such as name, address and date of birth are used without your knowledge to commit fraud. For example, they can be used to:

- take out credit in your name, such as a loan or credit card;
- take money from your bank account;
- apply for benefits in your name;
- buy goods in your name; or
- obtain documents, such as a driving licence or passport, in your name.

Identity fraud can affect your ability to get credit, such as loans and mortgages.

Investment scams

This is where fraudsters offer investments in goods and schemes that do not exist. You may be contacted out of the blue and told about opportunities to invest in special schemes that, for example, buy shares or precious metals and gems. Fraudsters can sound very knowledgeable and try to put pressure on you to make a quick decision. You could lose money if you pay the fraudsters and give away personal information that could be used for other types of fraud.

Loan scams

Loan scams are where fraudsters offer you a loan that does not exist. They approve your application, often very quickly, and then ask for an up-front fee. They may even explain that the fee is to cover insurance, or other costs. If you pay a fee to a loan scam, you will not receive the loan. You will lose money and any personal information you have given could also be used for other types of fraud.

Pension scams

A pension scam will try to get you to transfer the money in your pension to the fraudster. Fraudsters may contact you offering a free pension review and say that they can use a ‘loop hole’ to help you release your pension before age 55. They may also offer you a special ‘one-off’ investment opportunity to increase your pension if you transfer your funds quickly. You could lose your pension and in some cases also be left with a tax bill.

Prize draw or lottery scams

This is where fraudsters tell you that you have won a fake prize. Sometimes they even pretend to be from a well-known organisation. They may ask you to pay an up-front fee to release your prize, ring a premium rate telephone number, or give your bank account details and personal information. You could lose money if you pay the fee or ring the expensive phone number. Your personal information could also be used for other types of fraud.

Refund of council tax schemes

This is where someone contacts you out of the blue to say that you have been placed in the wrong council tax band. For a fee, they say that they can help you get a refund, and may even tell you how much you are owed. Some fraudsters pretend to be from your local council or even HM Revenue and Customs (HMRC). You could lose money if you pay the fee and give away personal information that could be used for other types of fraud.

Remember:

council tax

HMRC does not deal with council tax issues.

Preventing fraud

There are things that you can do to help protect yourself from fraud.

- Before you give anyone your personal information, such as your name, address and bank details, check who they are.
- If someone calls you and you are unsure whether they are genuine, hang up. Find their number from a statement or letter they have sent you or from the phone book. Call them back using that number. **Make sure that you wait at least 10 minutes before you call them back, or if possible use another phone.** This is because some fraudsters do not hang up when you do and try to block your phone line. It means you could still be speaking to them even when you think you are calling someone else, such as your bank or internet provider.
- Be careful of emails asking you to click on a link to confirm your personal information or bank details. Banks, HMRC and the police do not send emails asking you to do this.
- Think about what information you include on a social networking site, such as Twitter or Facebook. Don't add your full name, date of birth or address to your accounts. Don't share anything that you use as a password, such as your pet's name.
- Make sure your letter box is secure, and if you move house redirect your post with Royal Mail.
- Destroy and, where possible, shred any post showing your name and address, as well as any receipts showing your credit card details.
- Report missing or stolen documents to whoever issued them to you. If they are used by fraudsters there will be a record of what has happened.
- Use up to date anti-virus software and a firewall on your computer. These will help to prevent harmful programmes from taking information from your computer.
- Don't be tempted to download programmes, such as games, from sites that are not trusted. They may contain 'malware'.
- Take care when using public Wi-Fi. Wi-Fi allows you to connect to the internet. Many pubs, cafes and train companies offer free Wi-Fi to their customers. Do not access sensitive sites like your bank account when using this kind of Wi-Fi.

Information INFO

trusted sites

A trusted site is a website that you trust not to cause damage to your computer or take information from it.

If your anti-virus software is up to date you should get a warning about a site that is not trusted. Some sites might also be blocked.

For free information about being safe when you go online see Get Safe Online or Victim Support's Staying safe online.

- Sign up to Verified by Visa or MasterCard SecureCode if you are asked to when shopping online. Once you are registered, companies that use this service will carry out extra security checks when you shop online.
- Check your credit reference file regularly for any entries that you do not recognise. See the section **'Checking your credit reference file'** for more information.
- Make sure if you receive a bill or a receipt for something you have not ordered that you investigate further.
- If you are asked to invest in a scheme, look at **ScamSmart**. This is a tool set up by the **Financial Conduct Authority (FCA)**. It gives details about the risks linked to some investments and has a warning list of firms to avoid. See **Useful contacts** at the end of this fact sheet.
- If you are looking for a loan, it is important to check that the organisation you are dealing with is authorised by the **FCA**. See **Useful contacts** at the end of this fact sheet.
- If you are contacted out of the blue about your pension, do not give any personal information or agree to anything. Get free trusted advice first.
- Consider registering with **Action Fraud Alert**. This is free and sends you alerts about fraud and scams that may affect you. See **Useful contacts** at the end of this fact sheet.

Information: INFO

free pensions advice

Pension Wise offers free and impartial government guidance on pensions, including information on **How to avoid a pension scam**.

You can also contact **The Pensions Advisory Service** (TPAS) for free independent information and advice on pensions.

See **Useful contacts** at the end of this fact sheet.

Checking your credit reference file

Credit reference agencies hold information about credit agreements in your name, such as loans and credit cards, as well as details of organisations that have recently 'searched' your file. A 'search' is usually done by lenders when you (or someone pretending to be you) apply for credit.

There are three main credit reference agencies, Equifax, Experian and TransUnion. Get a copy of your credit reference file from all three agencies. You can ask for a copy under the **Data Protection Act 2018** for free. See **Useful contacts** at the end of this fact sheet.

Check the credit agreements and searches that are listed on your credit reference files. If you find an entry that you do not recognise then contact one of the credit reference agencies. They should contact the other two agencies to explain what has happened.

The credit reference agencies will need to contact the relevant creditor for permission to remove any fraudulent entries on your credit reference file. If you have any problems getting this information removed, **contact us for advice**.

If there is an entry that you do not recognise, see the section **'What to do if you have been a victim of fraud'**.

What to do if you have been a victim of fraud

Unfortunately, most people are only aware that they have been a victim of fraud when the money or goods have already been lost. **However, this is not always the case.** If you have recently spoken to someone, or responded to an email or text and think you have been scammed, there may still be time to stop any payments being made. Contact your bank or the relevant organisation immediately and explain what has happened. They may be able to put a stop on your accounts.

Contact your bank or creditor

If someone has taken out credit in your name, or taken money from your bank account without your permission, contact your bank or the creditor straight away. Explain what has happened, give them the crime reference number (if you have one) and ask them to investigate the matter. Any collection of the fraudulent debt should be put on hold while the matter is looked at.

You are **not** usually liable for money taken out in your name through identity fraud.

If money has been taken from your bank account or credit card without your permission then you will usually be entitled to a refund of any unauthorised payments. Tell the bank immediately because you may have to pay up to **£35** of any unauthorised payments taken before you notify the bank. You are not liable for any unauthorised payments taken after you tell the bank that your card has been stolen or that someone else has got hold of your security details.

If you have been tricked into making a payment and have given your card details to a fraudster, then you might not get your money back. **Contact us for advice.**

Extra advice:

refused a refund

If your bank refuses to refund unauthorised payments, they should tell you why. They can only usually refuse if:

- they can prove that you authorised the payments;
- they can prove you were at fault because you acted fraudulently or negligently; or
- you told them about the fraud **13 months** or more after the payment was taken.

If you are unhappy with the bank's response, **contact us for advice**.

Contact Action Fraud

Contact Action Fraud to report the fraud, see **Useful contacts** at the end of this fact sheet.

Action Fraud does **not** investigate the fraud, but they will:

- record what has happened;
- issue a crime reference number; and
- ask whether you want your details passed to Victim Support, a charity helping people affected by crime.

After you have reported the fraud, Action Fraud will pass details to the National Fraud Intelligence Bureau (NFIB). The NFIB will assess whether there is enough evidence to send it to the police or Trading Standards to investigate. You will then get an update on your report within **28 days**.

Not every report results in an investigation, but every report helps to build a clear picture. This helps to make the UK a more difficult place for fraudsters to operate in and helps to keep other potential victims safe.

Cifas

If you have been a victim of fraud consider contacting Cifas and signing up for their Protective Registration.

Cifas is a not-for-profit organisation and, if you sign up to their service, they will place a warning flag against your details. This tells any creditor using their information to carry out extra checks when your details are used to apply for credit or goods. For a small fee, Protective Registration aims to reduce the risk of further identity fraud. See **Useful contacts** at the end of this fact sheet.

Using Cifas does not affect your credit score but, due to the extra checks, it can make your credit applications take a little longer.

Advice:

protect yourself

If you have already experienced fraud you are still at risk from other attempts.

This is because as well as trying to commit fraud, some fraudsters also make money by selling your details to others.

Complaints

If you have been a victim of fraud and are unhappy with how a bank, creditor or credit reference agency has dealt with the matter then you can make a complaint.

You will need to complain to the organisation you are unhappy with first. Do this in writing and keep a copy of your letter. If you do not get a reply after eight weeks, or you are unhappy with the response, you can complain to the Financial Ombudsman Service (FOS). The FOS can look into your complaint independently. See **Useful contacts** at the end of this fact sheet.

If your complaint is about the information held on your credit reference file, you can also refer the matter to the Information Commissioner's Office under the **Data Protection Act 2018**. They can look at why a lender or credit reference agency has not corrected information on your file. See **Useful contacts** at the end of this fact sheet.

Useful contacts

Action Fraud
Phone: 0300 123 2040
www.actionfraud.police.uk

Cifas
Phone: 0330 100 0180 for Protective Registration enquiries
www.cifas.org.uk

Equifax
Phone: 0800 014 2955
www.equifax.co.uk

Experian
Phone: 0800 013 8888
www.experian.co.uk

Financial Conduct Authority
www.fca.org.uk/consumer
www.fca.org.uk/firms/financial-services-register to search the register

Financial Ombudsman Service
Phone: 0800 023 4567 or 0300 123 9123
Email: complaint.info@financial-ombudsman.org.uk
www.financial-ombudsman.org.uk

Get Safe Online
For free information about being safe online.
www.getsafeonline.org

Pension Wise
Phone: 0800 138 3944 to book a phone appointment
www.pensionwise.gov.uk/en

The Pensions Advisory Service
Phone: 0800 011 3797
www.pensionsadvisoryservice.org.uk

TransUnion (previously Callcredit)
Phone: 0330 024 7574
www.callcredit.co.uk

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk