

# FRAUD



FIRST PRINCIPLE

[norfolk.police.uk/firstprinciple](http://norfolk.police.uk/firstprinciple)  
[suffolk.police.uk/firstprinciple](http://suffolk.police.uk/firstprinciple)

## Top Tips

- If it sounds too good to be true - it probably is
- Always be suspicious of cold calls
- Ask a friend or colleague for a second opinion
- Never agree anything in haste
- Don't do business on the doorstep
- Look on the Action Fraud website <https://www.actionfraud.police.uk/>  
Tel 0300 123 2040
- Always keep your personal information secure.
- Store paper documents safely and never enter details onto a website if it is not secure (shown as a padlock or with https).
- Always dispose of personal documents by shredding

## PREVENT CRIME

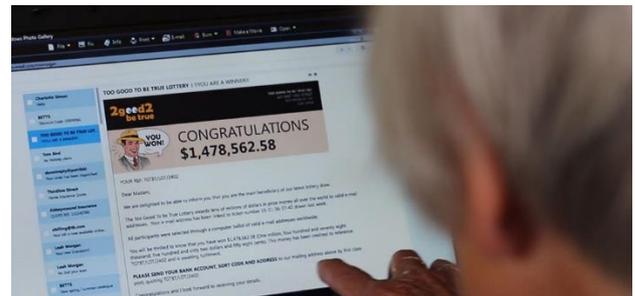
## PROTECT COMMUNITIES



**NORFOLK**  
CONSTABULARY  
*Our Priority is You*



**SUFFOLK**  
CONSTABULARY



**Fraud has become a common way for criminals to attempt to steal your money. This guidance note aims to make you aware of some common types of fraud together with tips to help you stay safe.**

**For more information look on the Action Fraud Website**

**Source of Information – Action Fraud**

## Pension Fraud

Pension fraudsters promise to convert pension benefits into cash before age 55



Criminals are believed to be fraudulently exploiting the pension liberation process in a number of ways. These include failing to advise members of the tax implications of receiving cash from their pension; failing to advise members of the full extent of fees to be paid in relation to any onward investment; falsely representing anticipated levels of returns when investments are either non-existent or incapable of providing such a return.

- The industry estimates that the current loss to the UK from this fraud type is £600 million.
- The scammers have a variety of tricks to catch you out. They may:
  - claim that you can access your pension pot before age 55
  - approach you out of the blue over the phone, via text message or in person door-to-door
  - entice you with upfront cash
  - offer a free 'pension review' or try to lure you in with so-called 'one-off' investment opportunities.

Check the facts before you make an irreversible decision. A lifetime's savings can be lost in a moment.

The Pensions Regulator's five steps to avoid becoming a victim of a pension scam:

1. Never give out financial or personal information to a cold caller
2. Check the credentials of the company and any advisers – who should be registered with the Financial Conduct Authority <https://www.fca.org.uk/>
3. Ask for a statement showing how your pension will be paid at retirement, and question who will look after your money until then
4. Speak to an adviser that is not associated with the deal you've been offered, for unbiased advice
5. Never be rushed into agreeing to a pension transfer.

### Resources

The Pensions Regulator has produced some resources for you to download to help prevent you becoming a victim.

- Individuals - For pension scheme members – how to spot a scam and protect yourself.
- Trustees - How pension scam models are changing and resources you can use when communicating to members.
- Business advisers - How pension scam models are changing and resources to help you to protect your members.

For more information about pension scams visit The Pensions Regulator website.

<https://www.thepensionsregulator.gov.uk/>

Before you sign anything, call The Pensions Advisory Service on 0300 123 1047

The HM Revenue & Customs website highlights the tax consequences of pension liberation to individuals.

If you have been a victim of this type of fraud, report it to Action Fraud by calling them on 0300 123 2040 or by using the online reporting tool.

## Police and Bank Scam

How does the scam work?

The offender calls the victim, purporting to be a police officer, and tells them they are investigating a fraud on their bank account and have someone arrested.



They might also claim to be from the victim's bank, again stating they are investigating fraudulent activity on their account. The offender asks for account information, including card, security and PIN numbers. Sometimes the offenders will ask victims to 'key in' their PIN number into the phone – the number is then captured by the offenders.

They may also ask the victim to withdraw a

large sum of cash from their bank or building society. If they make this request they will explain that the money is required as it needs to be forensically examined. They also instruct the victim not to tell the bank why they are withdrawing the money, giving the reason that the bank might be involved in the fraud.

The victim is then instructed to put the bank cards and/or money into an envelope and give them to a courier or taxi, which is sent to the house by the offenders to collect the items. If bank cards are collected they will be later used by the offenders to withdraw money.

In some cases, the victim might become suspicious and doubt the validity of what the caller is saying. If this happens, the offender will suggest they call the police via 999 or 101 or contact their bank in order that the victim can confirm the caller's identity.

However, what the victim doesn't realise is that the caller hasn't hung up so the line remains open, even if the victim hangs up, so the victim is put straight back through to the offender who will then pretend to be another person. This 'new' person will then validate the original caller's claims.

What should you do if you get a call?

If you are not happy with a phone call and are suspicious of the conversation you have with the caller then please end the call and report it to police.

- Remember, when reporting a suspicious phone call to police, wait at least five minutes before attempting to make the call

to ensure you're not reconnected to the offender.

- Alternatively, use a mobile phone or a neighbour's phone or test your landline by phoning a friend or relative first, to ensure you aren't still unwittingly connected to the offender.
- If you have concerns about your bank account, visit your local branch.
- The vital things to remember are that your bank and the police will NEVER:
  - ask for your bank account details or PIN number over the phone, so do not disclose these to anyone, no matter who they claim to be;
  - ask you to withdraw money and send it to them via a courier, taxi or by any other means; or
  - ask you to send your bank cards, or any other personal property, to them via courier, taxi or by any other means.

## Account Takeover

How does it work?

An account takeover can happen when a fraudster or computer criminal poses as a genuine customer, gains control of an account and then makes unauthorized transactions.



Any account could be taken over by fraudsters, including bank, credit card, email and other service providers.

Online banking accounts are usually taken over as a result of phishing, spyware or malware scams. This is a form of internet crime or computer crime.

Fraud has been committed if money has been lost. If fraud has been committed, report it to Action Fraud.

How to avoid an account takeover

- Keep track of your accounts
- Don't use a public Wi-Fi connection for banking
- Never ever reuse a password
- Use multi-factor authentication

## Investment Scam

An investment scam is when someone offers you a fake - but often convincing - opportunity to make a profit after they hand over a sum of money.



There are three main types of investment scams.

- A totally fictitious investment which doesn't exist.
- The investment exists but the scammer takes the money instead of putting it in the opportunity.
- The scammer pretends they're representing a legitimate and trusted investment group, but they're lying.

Investment scam warning signs

- Companies contact you out of the blue. This could be through a cold call, text, message on social media, email or brochure.
- They pressure you into making a rushed decision. This could be with a limited time offer, bonus or discount if you sign up before a deadline.
- They call or email you repeatedly or keep you on the line. This is to try keep you engaged so they can pressure you to make a rushed decision.
- It seems too good to be true. The old saying rings true - if they downplay the risks but the investment is high return, it could be an investment scam.

- They ask you to keep the investment quiet. The scammer might tell you the investment opportunity is just for you and ask you not to tell anyone.
- They're not registered on the FCA website. In the UK, a firm must be authorised and regulated by the FCA to do most financial services activities. See if they're registered with the FCA.

The FCA also has a warning list so you can check if you're dealing with a known scam.

You will likely be approached either through a cold call on your landline or mobile or via an email or text. The questionable investment could be advertised on social media or in a pamphlet.

## Bank Account Fraud

Bank account fraud has occurred if transactions you haven't made show up on your bank statement.

Bank account fraud could happen as a result of identity theft, when cards or bank account information has been stolen.

Protect yourself against identity fraud

- Don't throw out anything with your name, address or financial details without shredding it first.
- If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your full password, login details or account

numbers. Most banks will not approach their customers in this manner.

- If you are concerned about the source of a call, ask the caller to give you a main switchboard number for you to be routed back to them. Alternatively, hang up and call your bank back on the legitimate phone number printed on your bank statements.
- Check your statements carefully and report anything suspicious to the financial institution concerned.
- If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or credit card company.
- Don't leave things like bills lying around for others to look at.
- If you move house, always get Royal Mail to redirect your post.

<https://www.royalmail.com/personal/receiving-mail/redirection>

- Get regular copies of your credit report from a credit reference agency. 0300 123 9123

Notify your bank immediately if you see any unusual activity on your account.

## Plastic Card Fraud

Plastic card fraud involves the compromise of any personal information from credit, debit or store cards.

The personal information stolen from a card, or the theft of a card itself, can be used to commit fraud.



Fraudsters might use the information to purchase goods in your name or obtain unauthorised funds from an account.

Plastic card fraud can also include 'card not present' fraud, such as the use of a card online, over the phone or by mail order, and counterfeit card fraud.

Protect yourself against plastic card fraud

- Keep all your cards and financial details safe:
- look after your cards and card details at all times. Try not to let your card out of your sight when making a transaction
- check receipts against statements carefully. Contact your card company immediately if you find an unfamiliar transaction
- store your statements, receipts and financial documents safely and destroy them, preferably using a shredder, when you dispose of them
- sign any new cards as soon as they arrive
- cut expired cards through the magnetic strip and chip when replacement cards arrive.

Secure your PIN:

- memorise your PIN and destroy any paper notification as soon as you receive it

- ensure that you're the only person that knows your PIN. Never write it down or record it. Your bank or the police will never phone you and ask you to disclose your PIN
- when entering your PIN, use your free hand and your body to shield the number from prying eyes or hidden cameras. If you think someone has seen your PIN or if you want to change it to something more memorable, you can change it at a cash machine (ATM) or by contacting your bank.

Take care when using cash machines:

- put your personal safety first. If someone makes you feel uncomfortable, cancel the transaction and use a different machine
- if you spot anything unusual about the cash machine, or if there are signs of tampering, don't use it. Report it to the bank concerned immediately
- be alert. If someone is crowding or watching you, cancel the transaction and go to another machine. Don't accept help from seemingly well-meaning strangers and never allow yourself to be distracted
- once you've completed a transaction, put your money and card away before leaving the cash machine. If the cash machine doesn't return your card, report its loss immediately to your card company. Destroy or preferably shred your cash machine receipt, mini-statement or balance enquiry when you dispose of them.

Contact your bank immediately if you think your card or personal information has been compromised.

## Romance Fraud

What is it?

When you think you've met the perfect partner through an online dating website or app, but the other person is using a fake profile to form a relationship with you. They're using the site to gain your trust and ask you for money or enough personal information to steal your identity.



Protect yourself

- Avoid giving away too many personal details when dating online. Revealing your full name, date of birth and home address may lead to your identity being stolen.
- Never send or receive money or give away your bank details to someone you've only met online, no matter how much you trust them or believe their story.
- Pick a reputable dating website and use the site's messaging service. Fraudsters want to quickly switch to social media or texting so

there's no evidence of them asking you for money.

### Spot the signs

- You've struck up a relationship with someone online; they're asking a lot of personal questions about you, but they're not interested in telling you much about themselves.
- They invent a reason to ask for your help, using the emotional attachment you've built with them. Your relationship with them may often depend on you sending money.
- Their pictures are too perfect – they may have been stolen from an actor or model. A reverse image search can find photos that have been taken from somewhere else.

### How it happens

The majority of accounts on dating websites are genuine people looking for romance, but fraudsters may try to contact you by making fake profiles, getting in touch and building what feels like a loving relationship.

Once a fraudster using a fake dating profile is confident that they've won your trust, they will tell you about a problem they're experiencing and ask you to help out by sending money.

They may have arranged to visit you, but need money to pay for the flight or visa. They may tell you everything has been booked but their ticket has been stolen, and you need to send money quickly to get them on the next flight.

Alternatively, they may prey on your sympathies, telling you a family member or someone else they are responsible for is ill and they need money for medical treatment.

Once you send them money, the fraudsters will keep coming back and invent new reasons to send them more.

### How to report it

It can be embarrassing to feel tricked into thinking you've formed a relationship online, but Action Fraud can take a report in confidence. Report it online or call 0300 123 2040.



### How can you help?

- Please share this information with your older relatives and friends: this crime has a devastating effect on people and we need to raise awareness to prevent further people becoming victims.
- Report any calls you believe are suspicious as we may be able to trace where the calls are originating from. Please remember, to wait at least five minutes before calling police or use a mobile or neighbour's phone.
- Report suspicious activity at cash points. If

you see someone spending a long time at a cashpoint, using a number of different cards and have a hood up or their faces covered, contact police immediately. Often offenders will use cashpoints in the early hours.

You can also watch a video from YouTube below, provided by Action Fraud and entitled, 'The Devil's in Your Details':

<https://www.youtube.com/watch?v=0N4MgKN3pkE>

These are just some of the fraud types we have experienced in Norfolk and Suffolk recently. Below is a list of fraud types. Information about these is available on the Action fraud website.

<https://www.actionfraud.police.uk/a-z-of-fraud>

Abuse of position of trust  
Accommodation addresses  
Accommodation fraud  
Account takeover  
Action Fraud Remit  
Advance fee fraud  
Anti-competitive behaviour  
Application fraud  
Asset misappropriation fraud  
Auction fraud  
Bank account fraud  
Bank card and cheque fraud  
Bankruptcy-related fraud  
Benefit fraud  
Betting fraud

Bogus tradesmen fraud  
Boiler room fraud  
Bond fraud  
Botnet-related fraud  
Business directory fraud  
Business opportunity fraud  
Business trading frauds  
Call centre fraud  
Career opportunity scams  
Cash point fraud  
Charitable publication scams  
Charity donation fraud  
Charity fraud  
Cheque fraud  
Cheque overpayment fraud  
Clairvoyant scams  
Click fraud  
Companies – fraudulent  
Computer hacking  
Computer Software Service frauds  
Corporate fraud  
Corporate services fraud  
Council tax fraud  
Counterfeit cheque fraud  
Counterfeit gift certificates  
Counterfeit goods fraud  
Courier fraud  
Courier scam  
Credit card fraud  
Cryptocurrency investment fraud  
Customer fraud  
Cyber  
Debit and credit card fraud  
Debit card fraud  
Distributed Denial of Service (DDoS)  
Distribution Fraud  
Domain name scams

Door-to-door sales fraud  
 Doorstep electricity meter credit scams  
 Doorstep fraud  
 Electricity scam  
 Employee fraud  
 Employment fraud  
 Energy top-up scam  
 Exploiting assets and information  
 Facility takeover  
 False accounting fraud Financial investment  
 Fixed line fraud  
 Fraud enabling activities  
 Fraud recovery fraud  
 Fronting  
 Gambling fraud  
 Goods sold as investment  
 Government agency scams  
 Health in Pregnancy Grant fraud  
 Health scams  
 Hedge fund fraud  
 Holiday club fraud  
 Holiday fraud  
 Identity fraud and identity theft  
 Impersonation of officials  
 Individual fraud  
 Inheritance fraud  
 Insider information  
 Insolvency fraud  
 Insolvency-related fraud  
 Institutional investment fraud  
 Insurance broker scams  
 Insurance fraud  
 Intellectual property fraud  
 Internal fraud  
 Internet auction fraud  
 Internet dialler scam  
 Investment fraud  
 Invoice scams  
 Land banking scams  
 Life assurance takeover  
 Loan repayment fraud  
 Loan scams  
 Lottery fraud  
 Lottery scams  
 Mail boxes and multiple post redirections  
 Malware and computer viruses  
 Mandate Fraud  
 Market manipulation  
 Marketing materials  
 Mass marketing fraud  
 Medical scams  
 Miracle health scams  
 Mobile phone fraud  
 Money muling  
 Mortgage fraud  
 Non-domestic rate fraud  
 Office supply scams  
 Online fraud  
 Online shopping fraud  
 Patient charge evasion  
 Payment fraud  
 Pensions scams  
 Personnel management fraud  
 Phishing  
 Phoenix company fraud  
 PIN entry devices  
 Plastic card fraud  
 Ponzi schemes  
 Premium rate phone line scams  
 Prime bank guarantee fraud  
 Prize draw scams  
 Procurement fraud  
 Property fraud  
 Property investor scams

Proxy servers  
Psychic scams  
Public funding and grants  
Public sector service provision  
Publication fraud  
Pyramid scheme fraud  
Racing tipster scams  
Receipt fraud  
Recruitment scams  
Rental fraud  
Romance fraud  
Romance scams  
Share sale and investment fraud  
Shopping fraud  
Short and long firm fraud  
Sign up to Action Fraud Alert  
Slimming cures scams

Smishing  
Spam emails  
Store card fraud  
Sweepstake scams  
Tabnapping  
Tax fraud  
Telecomms  
Telecommunications frauds  
Ticket fraud  
Ticket scams  
Timeshare fraud  
Travel and subsistence fraud  
Vehicle matching scams  
Vishing  
Website domain name scams  
West African letter fraud  
Work from home scams

## First Principle: Related links

Check out all of our Crime Prevention information using the following links or by using the QR code to take you to the First Principle Pages Alternatively go to our website at <https://www.suffolk.police.uk/> and look in the 1<sup>st</sup> Principle A-Z of Crime Prevention.

Allotment Security  
Anti-Social Behaviour  
ATM Security  
Beach Hut Security  
Boat Security  
Building Site Security  
Business Security  
Caravan Security  
Caravan Storage  
Card Security  
Catalytic Converters  
Church Security  
Cold Callers  
Commercial CCTV  
Counterfeit Banknotes  
County Lines Advice for Landlords  
Cyber Crime  
Cycle Security  
Dangerous Dogs  
Dog Fouling  
Dog Theft  
Domestic CCTV  
Domestic Violence  
Farm Security  
Fraud Prevention  
Grooming  
Hate Crime

Heating Oil  
Home Improvements  
Home Security  
Home Security for Tenants  
Horses and Stables  
Keyless Vehicles  
Key Safe Security  
Lock Snapping  
Mopeds and Scooters  
Motorcycle Security  
Neighbour Disputes  
Occupiers Liability  
Personal Security  
Power Tool Security  
Products Brochure  
Rural Crime  
Security Alarms  
Sheds and Garages  
Social Media  
Social Media for Parents  
Suspicious Behaviour  
Shoplifting  
Taxi Driver Safety  
Vehicle Security  
Windows and Doors



### Other Links you might find helpful

Ask the Police  
Secured by Design  
Sold Secure

Crimestoppers  
0800 555 111

Victim Care  
0300 303 3705