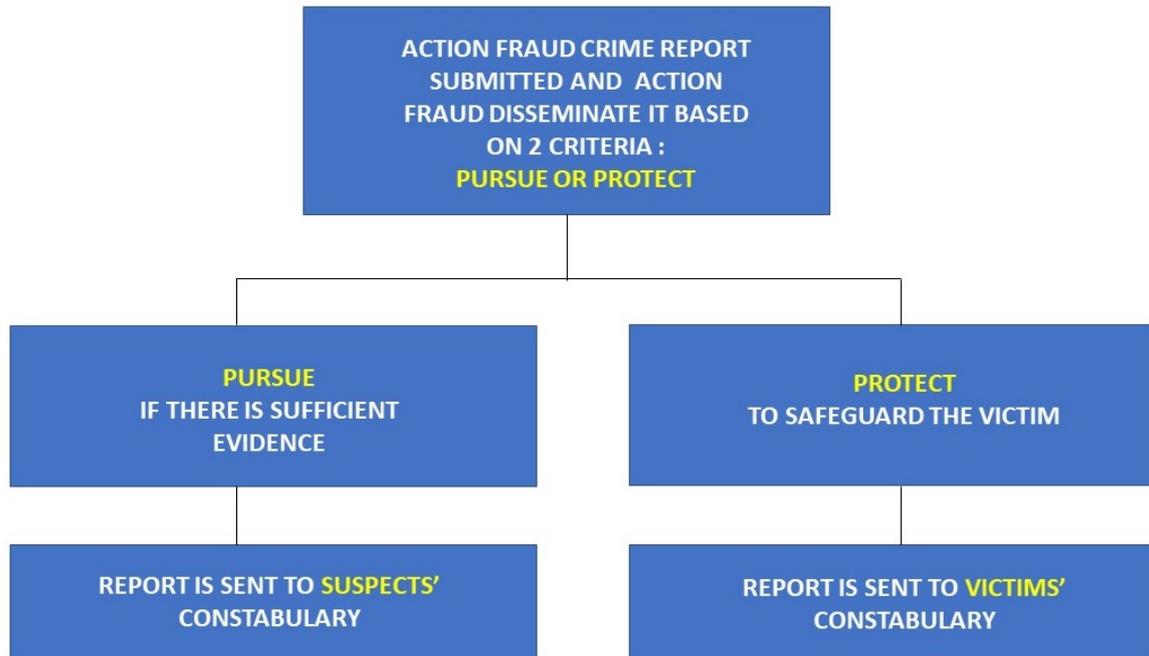


This article explains what you should do if you think you've been a victim of fraud and how Action Fraud operates. All cases of fraud should be reported to [Action Fraud](#), even if it has been reported to the police, as the reference number they provide is the crime number which will be required when contacting any other organisations going forward.



Action Fraud is the UK's national reporting centre for fraud and cybercrime and each week, every police force within England and Wales (Scotland does not use this process) are notified of reports submitted within their force area.

Action Fraud are responsible for disseminating the report to Police Forces as either a "pursue" or a "protect". This is **not** the decision of the force in question, who action it as instructed by Action Fraud. So, for example, if a fraud has been committed and the **suspect** is based in Manchester, Action Fraud will pass it to GMP to **pursue** (investigate), if the **victim** is in Lancashire, Action Fraud will pass it to Lancashire to **protect** (safeguard).

Action Fraud will respond direct to all individuals who have submitted a report, advising of their decision and any action taken.

Lancashire Constabulary receive approximately 150 victim cases from Action Fraud weekly, the majority of which although they may be considered fraudulent by the victim, are actually under the jurisdiction of other governing organisations. We understand that falling foul of a fraud can be a traumatic experience, so when triaging victim cases for safeguarding, we will

contact the individuals concerned and point them in the right direction, whilst also providing whatever emotional and practical help we can to assist them through a very difficult time.

The most common complaints are identified below. The links provide information about the organisation as well as their contact details:

<b>1.</b>	<b>Bank</b> If you suspect that your bank account has been hacked or compromised, then always speak to your bank in the first instance. A <a href="#">Banking Protocol</a> has been introduced to help protect vulnerable customers from certain scams.
<b>2.</b>	<b>Door-to-door Sales &amp; Rogue Tradesmen</b> Our advice would be to never engage with random people who cold call you. Always carry out due diligence and never be panicked into making a snap decision. Check out the product, the company, the person. If you are unhappy with a product or any work undertaken, then contact: <a href="#">Citizens Advice</a> (who can provide advice and forward onto Trading Standards) <a href="#">Trading Standards</a> These individuals can be very persistent and intimidating. If this is the case then report them to 101 or, if feeling threatened, ring 999.
<b>3.</b>	<b>Abuse of Power of Attorney</b> Attorneys are placed in positions of trust, making important decisions which impact the donor's day-to-day lives. Unfortunately, they may underestimate the legal duties placed upon them and can become complacent. There is also a danger that they may exploit the donor's trust by mispending money, failing to keep proper accounts and even using the money to benefit themselves. <a href="#">Office of the Public Guardian.</a>
<b>4.</b>	<b>Consultants or companies</b> If you are unhappy with consultants that you have employed or discover that your address is being used to front a company unknown to you, then contact: <a href="mailto:enquiries@companieshouse.gov.uk">enquiries@companieshouse.gov.uk</a> .
<b>5.</b>	<b>Communications</b> Ofcom is the regulator for the communications services that we use and rely on each day such as broadband, home phone, mobile services, TV and radio. <a href="#">Ofcom</a>

6.	<p><b>Energy Providers</b></p> <p>Ofgem is Great Britain's independent energy regulator. They work to protect energy consumers, especially vulnerable people, by ensuring they are treated fairly and benefit from a cleaner, greener environment.</p> <p><a href="#">Ofgem – the energy regulator for Great Britain</a></p> <p><a href="#">Energy Ombudsman</a></p>
7.	<p><b>Identity Theft</b></p> <p>If you think you are a victim of identity theft or fraud, act quickly to ensure you are not liable for any financial losses.</p> <ul style="list-style-type: none"> <li>• Report all lost or stolen documents, such as passports, driving licences, credit cards and cheque books to the organisation that issued them.</li> <li>• Inform your bank, building society and credit card company of any unusual transactions on your statement.</li> <li>• Request a copy of your credit file to check for any suspicious credit applications.</li> <li>• Report the theft of personal documents and suspicious credit applications to the police and ask for a crime reference number.</li> <li>• Contact CIFAS (the UK's Fraud Prevention Service) to apply for protective registration. Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.</li> </ul> <p><a href="http://www.cifas.org.uk">www.cifas.org.uk</a></p>
8.	<p><b>Corrupt Financial Advisors</b></p> <p>Do not act in haste. Always take time to think about or "sleep on" a financial decision. An attempt to rush you should be a red flag. If there's a good opportunity today, it won't go away tomorrow. Don't be afraid to walk away if an offer doesn't seem right.</p> <p><a href="#">Financial Conduct Authority</a></p>
9.	<p><b>Probate Queries</b></p> <p><a href="#">What is probate - GOV.UK (www.gov.uk)</a></p>
10.	<p><b>Breach of Data Protection</b></p> <p><a href="#">Information Commissioner's Office (ICO)</a></p>
11.	<p><b>Charity Donation Fraud</b></p> <p>Fraudsters may take advantage of your generosity when giving to charity, especially in the current economic climate. They may claim to be raising money for</p>

a fake charity or impersonate a well-known charity. Most fundraising appeals are genuine, so the risk of fraud should not put you off giving to charities. However, you should be vigilant and make sure you are giving safely to legitimate organisations. The [Fundraising Regulator](#) and [Charity Commission for England and Wales](#) advise you to pause and check before donating. This includes:

- Check the charity name and registration number at [uk/checkcharity](#).
- Also check the Fundraising Regulator's online Directory to see if a charity has committed to good fundraising practice at [org.uk/directory](#).
- If you're still unsure about giving, always ask the organisation for more information. Legitimate causes will be happy to respond and answer your questions.

If you are in any doubt about the validity of the person you are dealing with, then report it to the relevant governing organisation. However, if you suspect fraudulent activity then report it to [Action Fraud](#).

I hope that you found this useful. Until our next newsletter stay safe and be alert. A pdf version is attached for those who need to alter the size of the text for ease of reading.

Best wishes,

The Fraud Triage Team