

TITLE	Action Fraud – Urban Myths
SUBTITLE	FRAUD
DIRECTORATE	ECD

1) Action Fraud investigates fraud.

Action Fraud does not carry out the investigations into fraud, and does not have the requisite powers to do this. Its remit is to take reports of fraud, which are then sent to the National Fraud Intelligence Bureau (NFIB), 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.

Investigation and enforcement are not the only ways to fight fraud; taking steps to prevent it from happening in the first place is just as important. Reports made to Action Fraud can lead to the disruption of telephone lines and websites linked to fraudulent activity, or working with banks to request the closure of accounts linked to crime. From April 2016 to March 2017 the NFIB disseminated 46,019 reports for further action on intelligence, prevention or victim care and submitted 170,856 requests to partners to close bank accounts, websites and phone numbers suspected of facilitating fraud.

2) A victim has to be defrauded of a certain amount, otherwise their fraud won't be investigated.

This is not the case, a report of fraud will not be ruled out for investigation purely on the basis of the amount lost. When a fraud report comes in to the NFIB, an assessment matrix is used to identify those reports that meet the required investigative threshold, and a number of factors influence this. These include whether there are any linked reports from across the millions of reports made to the NFIB and whether money has been transferred to a UK bank account. Where the fraud amount **is** relevant is when the reported loss is over £100,000; these reports are automatically reviewed.

Other cases that result in automatic review include where the victim is vulnerable and in need of immediate support – the assessment process looks for triggers that may mean a victim is vulnerable.

3) If a fraud can't be investigated, the victim has wasted their time reporting it.

Action Fraud is the only national reporting system in the world, enabling data matching across all crime reports and reports provided by private and public sector partners. Recording fraud in this way and sharing intelligence via a single hub means that crime networks can be targeted effectively and that police resources are used efficiently, with similar cases from across the UK being sent

to a single force. Even when a report of fraud cannot be investigated, the data supplied can help to build an ever more accurate picture of fraud networks and trends, increasing the likelihood of positive outcomes in future. This information can also be used for the prevention of fraud, such as disrupting telephone lines and websites linked to fraudulent activity, or requesting the closure of accounts.

4) Forces should only receive fraud packages if the victims are residing in their force area.

Fraud is unique in that it can span numerous victims based in different locations across the country or even in different parts of the world. It is sometimes easier to specify one particular location for a **suspect**, rather than the victims. Therefore, forces may also receive fraud packages if it is the suspect who resides in their force area, rather than particular victims.

5) Fraud is a victimless crime.

A common misconception is that fraud is a victimless crime, or that it's not as serious as other crimes. This is not true. Fraudsters are often part of serious organised criminal gangs, who use the money to fund other crimes such as human trafficking, illegal firearms trade and terrorism.

In addition, fraud has repercussions for everyone, whether or not they are a direct victim of the crime. In 2016, the estimated cost of fraud to the UK was £193bn a year, though this is likely to be higher. That money has to be repaid somehow, which means that the cost of products and services increases for everyone.

Fraud can affect everyone, not just banks and other businesses.

6) The definition of vulnerability is different when it comes to fraud, as the impact on people isn't as severe.

The definition of vulnerability is the same for all forms of crime, it is no different for fraud. According to the NPCC, "A person is vulnerable if, as a result of their situation or circumstances they are unable to take care of, or protect themselves or others, from harm or exploitation".

However, there is a difference in terms of reporting a fraud crime; when a victim reports to Action Fraud, they are asked to self-identify if they consider themselves to be vulnerable.

7) It is mainly older people who fall victim to fraud and cyber crime.

This is not true. Anyone can fall victim to fraud and cyber crime in one of its many guises. What is true is that with all of the types of fraud and cyber crime, different demographic groups can be more susceptible than others to a particular kind. For example, young people are more likely to fall victim to binary options fraud or

ticket fraud, whereas an older age group is more likely to be a victim of targeted investment scams carried out by telephone.

8) Fraud reports can't be taken at front desk or over the phone, they all have to go via Action Fraud.

Victims of fraud can still go to a front desk or report a fraud over the phone. In these cases, officers or front office staff will provide assistance to victims in reporting fraud via Action Fraud. They will also triage the crime, and if the fraud is currently taking place, it will be treated as a call for service and a local police force will handle this.

9) Fraud is mainly perpetrated by criminals overseas, therefore there's nothing we can do to stop the offences.

Although UK police forces cannot carry out arrests in another jurisdiction, it is still possible to disrupt fraudulent websites or bank accounts based overseas. UK forces can also liaise with forces in other countries to stop fraud occurring or target offenders.

10) CoLP is a private police force funded by industries such as banking to tackle fraud

The City of London Police is not a private police force, it is one of the 43 territorial forces in England and Wales, and is Home Office and local authority funded. It provides policing services to the geographical area of the City of London, the Square Mile. In addition, a large part of the force's work is combatting fraud; it is the national policing lead for economic crime. As part of this work, there are some units within the Economic Crime teams that receive external funding, for example, the Insurance Fraud Enforcement Department (IFED), a specialist police unit dedicated to tackling insurance fraud. This unit is funded by the Association of British Insurers (ABI) and Lloyds of London members. IFED acts with operational independence while working closely with the insurance industry.

11) Fraud victims cannot report to their local force any more and must report to Action Fraud instead.

This is not true; victims can still report fraud to their local force. When this happens, the force will need to assess whether the victim requires a "call for service". This can occur when: an offender has been arrested for a fraud offence; the offender is committing or has recently committed a fraud offence at the time; or the suspect is known and police could locate them with the details provided; or have sufficient details to apprehend an offender.

Under the examples above, the local force will deal with the report and record it on both Action Fraud and their own crime management systems. However, in most cases and where there is not a "call for service", victims reporting fraud to

their local force can be advised to report to Action Fraud via the website www.actionfraud.police.uk or by telephoning 0300 123 2040. Where a force thinks a victim is vulnerable, they should assist them in making a report to Action Fraud.

Where fraud can be reported to Action Fraud rather than a local force, this provides additional value to policing by:

- shifting call demand from 999 and 101 away from forces
- saving forces time, resources and money
- providing expert help and support to victims of fraud and cyber crime
- providing a centralised way of reporting with a database that contains millions of high quality intelligence and crime reports relating to fraud and cyber crime.

12) Only stupid, gullible people fall victim to fraud.

Anyone can be a victim of fraud, there is no one type of person who is more likely to be a victim. ONS figures released in July this year revealed that people are more likely to fall victim to fraud or cyber offences than any other crime.

Fraudsters use a variety of different methods to target people, and these can be extremely sophisticated and convincing. There is no need to be embarrassed or stay silent about being a victim of fraud; what does matter is reporting the fraud to Action Fraud to increase understanding of the issue and to help prevent the same thing happening to others.