# Guidance Document

# Fraud – Calls for Service (CFS)

Action Fraud is the UK's national reporting centre for fraud and cybercrime. In the vast majority of cases, reports of fraud and cybercrime are completed via the Action Fraud website or Action Fraud call centre. There are, however, occasions when it is expedient for police forces to act immediately in response to the report of a fraud or cybercrime. These incidents are identified as Calls for Service (CFS).

The following headings provide guidance to police forces to explain what constitutes a Call for Service (CFS) and advice in relation to recording these incidents.

## Call for Service Criteria and Incident Recording

- Offences where offenders are arrested by the police;
- Where there is a CFS to the police and the offender 'is committing' or has recently committed (at the time of the CFS) all fraud types;
- The suspect is known and is a local suspect

A 'local suspect' is defined as where, through viable investigative leads:

- Police can or could locate the suspect with the details provided, or;
- Have sufficient details to apprehend an offender

'Recently Committed' should be interpreted using a common sense approach and dealt with on a case-by-case basis. The principle question for the force to answer is 'does the incident require an immediate response?'

'Local' has its everyday meaning (including a delivery address) and has been used to ensure that, as with any other type of crime, where there are local viable investigative leads, police should consider the crime for investigation. Local is not necessarily exclusive to a force's geographical area.

Where a CFS is apparent, police will create their own case management record according to local procedures and will record the offence at Action Fraud using the Expert Reporting Tool.

## What if the incident does not meet CFS criteria but the victim is vulnerable?

Policing recognises the need to identify and support vulnerable victims of crime. The College of Policing defines vulnerability as: *'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.'*

All forces have processes in place to identify vulnerability at point of contact and at subsequent points thereafter. Care should be exercised by forces when resources are deployed on the basis of vulnerability where it concerns the reporting of fraud or cybercrime. CFS protocols will still be applicable. We recommend an investigation should only be commenced if the attendant CFS criteria are met.

The NFIB Crime Transfer Process 2019 confirms:

**Vulnerable victim**:

- Police will take details of the allegation
- Record the fraud onto Action Fraud providing the victim with the NFRC number and password **OR** assist the victim in reporting it to AF themselves.
- Record dealing with a 'Vulnerable' person in line with your force policy and provide safeguarding as appropriate.

**Non Vulnerable Victim:**

- Advise the victim to report their fraud to Action Fraud
- There is **no need** to record this onto a local crime management system.

In both the above scenarios there is no obligation on the Force to undertake any further investigation, other than assisting, if appropriate, with reporting the allegation to Action Fraud. Local force policy should be followed in respect of recording the vulnerability assessment.

## What if the incident does not meet CFS criteria but involves a vehicle and/or plant?

Allegations of fraud made to a force involving Police National Computer (PNC) registered vehicles or plant will be reported by the receiving force to Action Fraud on behalf of the victim. The force will in addition be responsible for recording the appropriate report (LOS, interest etc.) for the vehicle / plant onto the PNC.

An investigation should only commence if the 'Call for Service' criteria are met.

## What if the incident does not meet CFS criteria but there is the potential to secure evidence?

Where contact is made with a police force to report a fraud or cyber offence consideration should be given to the securing and preservation of evidence, notwithstanding whether the matter is subsequently referred directly to Action Fraud, or is dealt with as a CFS by the force. This would include completing action with regards to the following;

1. Seizure of material that may not be available at a later date i.e. CCTV or forensic evidence.
2. Where funds are at risk. Example – victim informs you that the funds are still in the recipient's account as advised by suspect's bank but they require police intervention to freeze the account.

## Calls for Service Flowchart


Call for serv.pdf

## Handling Instructions

This document may be circulated in accordance with the protective security marking shown below and caveats included within the report. This document is marked as **OFFICIAL**. The information contained in this document is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership / handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the General Data Protection Regulation 2018 and the Data Protection Act 1998.

## Administration

| | |
|---|---|
| Type of Document: | Guidance |
| Version: | 1.0 |
| Effective Date: | September 2019 |
| Review Date: | September 2020 |
| Owner: | City of London Police |
| Approved by: | Det. Supt. Alex Rothwell |
| Further Information: | National.CoOrdinatorsOffice@cityoflondon.pnn.police.uk |