

# **Fraud Recording, Allocation and Investigation**

---

## **Policy & Procedure**

**Bedfordshire Police**

**April 2018**

**IMPLEMENTED:** 3<sup>rd</sup> April 2018

**REVIEW DATE:** April 2020

**POLICY OWNER:** Director of Intelligence

**APPROVED BY:** DCI Henderson

**PROTECTIVE MARKING:** Not Protectively marked

**IS THE POLICY**  New  Revised

**IF REVISED, PLEASE COMPLETE TABLE BELOW**

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)
1	19/03/18	Draft version after receipt from GMP	Sean O'Neil
2	24/04/18	Draft version after initial consultation	Sean O'Neil
2.1	24/04/18	Approved version DI Tilling Cyber Hub	Richard Tilling
2.2	24/04/18	Ammended version DCI Henderson Cyber Hub	Julie henderson

---

## Table of Contents

1. Introduction and Background.....	1
2. Scope.....	1
3. Roles & Responsibilities.....	1
4. Terms and Definitions .....	3
5. Procedure .....	3
6. Associated Documents.....	6
7. Consultation & Statutory Compliance .....	6
7.1 Consultation .....	6
7.2 Statutory Compliance.....	7
7.2.1 Data Protection Act (1998).....	7
7.2.2 Freedom of Information Act (2000).....	7
7.3.3 Equality Act 2010 .....	7
8. Appendices .....	7

---

## 1. Introduction and Background

The document outlines the procedure for the recording, allocating, and investigation of fraud offences. This follows a review into the effectiveness of current fraud investigations and the commencement of the Signpost victim hub.

---

## 2. Scope

This policy & procedure is aimed at :

- Crime Investigation Team (CIT)
- Crime Recording Unit; and
- General public (Allocation & Investigations only)

---

## 3. Roles & Responsibilities

### Call Takers

If you are the first responder dealing with a report of a fraud crime you should:

Consider if the person reporting should be referred to their bank/financial institution OR Action Fraud. An email should be sent to cyberprotect (beds) to allow the victim to be contacted and given cyber protect advice.

If the person reporting is vulnerable, meets the 'call for service' criteria, or the property stolen during the fraud is something that requires circulation on the PNC you should record a STORM log and a police officer should be allocated to deal with the report. (See Fraud Reporting Advice document )

### Initial Investigating Officer - Response/Community officer

If you are the first responder dealing with a report of a fraud crime on division, you should:

Consider if the person reporting should be referred to their bank/financial institution OR Action Fraud. If the person reporting is vulnerable or meets the 'call for service' criteria you should then:

- Conduct a thorough initial investigation. This will include taking statements and securing all available evidence including CCTV.
- Consider making an arrest if the offender is immediately available, and it is in the best interests of the investigation. In such cases, advice and assistance can be obtained from officers within the Cyber Hub, telephone ext. 2854.

- Submit crime report, a copy of all statements and supporting documentation, with the crime reference number via Crime Bureau/Athena IMU.
- Ensure that if the fraud crime has involved the use of the internet or a computer that the report is marked as a 'cyber crime'.
- Notify the victim that all reports of fraud are recorded by Action Fraud who will pass the details provided to the National Fraud Intelligence Bureau. Action Fraud and the National Fraud Intelligence Bureau are governmental organisations tasked with the recording of all fraud reported in England & Wales. Bedfordshire Police will pass information via the Crime Recording Unit to Action Fraud on the victim's behalf.

## Crime Recording Unit

You should send all relevant fraud cases, where possible, to the fraud & cyber security advisors at [cyberprotect@bedfordshire.pnn.police.uk](mailto:cyberprotect@bedfordshire.pnn.police.uk). A triage process will then be undertaken to evaluate the report, prior to allocation.

Ensure that if the fraud crime has involved the use of the internet or a computer that the report is marked as a 'cyber crime'.

All 'call for service' reported fraud crimes shall be reported to Action Fraud and the allocated Action Fraud crime number should be added to the Bedfordshire Police crime report.

## Fraud Triage Desk, [fraud & cyber security advisors]

You should evaluate all fraud cases in accordance with the guidance, 'Assessment Criteria for Fraud Investigations' (see section 5).

All reports of fraud screened in and accepted for secondary investigation will be investigated by CIT or Cyber Hub (Cyber Dependent Crime) or other resource as agreed by agreement with DI Cyber Hub & DI CIT.

Any allegation of fraud that is considered as complex and/or is clearly being committed by an Organised Crime Group (OCG) should be discussed with the ERSOU Regional Financial Investigation Unit. If they are in agreement that they are likely to accept it, the crime should be presented by the OIC to be assessed by the FTTCG. Any fraud being committed by an OCG will also be referred to ERSOU for consideration. With the agreement of the FTTCG the case will be presented at the RIG (Regional Intelligence Group) who will consider accepting ERSOU ownership.

All fraud of this type screened in for secondary investigation will be investigated by CIT officers, Cyber Hub officers, or ERSOU.

You should ensure that all fraud reports are recorded at the National Fraud Intelligence Bureau. See Action Fraud Referral Process appendix.

## 4. Terms and Definitions

Action Fraud – National Fraud Reporting Centre  
NFIB – National Fraud Intelligence Bureau  
PNC – Police National Computer  
OCG – Organised Crime Group  
FTTCG – Force Tactical & Tasking Co-ordination Group

---

## 5. Procedure

### Reporting a fraud – Frauds involving cheque, plastic cards or online bank accounts

Account holders attempting to report cheque, plastic card or online bank account fraud offences at police stations will be asked in the first instance if they have been specifically told to do so by their Financial Institution. If they have, they will be referred to the Action Fraud contact centre. If they have not, they will be told to contact their Financial Institution who will deal with the account holder. It is not necessary to record a crime related incident.

If the Financial Institution wishes an account holder to report the crime, the Financial Institution will give the account holder a reference number for Action Fraud – either in the form of a letter or verbally. In this case, the account holder will be asked to report it to the Action Fraud contact centre.

Where account holders with reference numbers attend the police station they should be referred to the Action Fraud contact centre.

Reporting a fraud –

Unless the circumstances fall into one of the below criteria, a person reporting a fraud should be directed to Action Fraud, personal details and brief circumstances should be obtained to allow the cyber protect team to contact the victim and give protect advice:

- Vulnerable victim
- Meets 'call for service' criteria
- Property stolen during the course of the fraud is suitable for circulation on the PNC.

### Allocation & Investigation

The decision on whether to investigate an allegation of fraud lies solely with the police. In making that decision, a number of factors must be considered, including the nature of the offence, resources available, the potential success of the investigation, the vulnerability of the victim and the impact of the crime.

All fraud allegations will be assessed by the Fraud Triage/Assessment Desk, Cyber protect via email [cyberprotect@bedfordshire.pnn.police.uk](mailto:cyberprotect@bedfordshire.pnn.police.uk).

In cases where the crime is screened in for further investigation, the crime will be allocated to the CIT or the Cyber Hub or other divisional resource as agreed by the CIT DI.

The exception to this will be offences of making off without payment and other minor fraud offences detected at source which will continue to be dealt with by Community officers or the initial attending officer.

Any allegation of fraud that is considered as complex and/or is clearly being committed by an Organised Crime Group (OCG) should be discussed with the ERSOU Regional Financial Investigation Unit. If they are in agreement that they are likely to accept it, the crime should be presented by the OIC to be assessed by the FTTCG. Any fraud being committed by an OCG will also be referred to ERSOU for consideration. With the agreement of the FTTCG the case will be presented at the RIG (Regional Intelligence Group) who will consider accepting ERSOU ownership.

All fraud of this type screened in for secondary investigation will be investigated by CIT officers, Cyber Hub officers, or ERSOU.

This policy takes into account Bedfordshire Crime Investigation Policy C003. In terms of allocation, SCIT are responsible for the majority of fraud investigations.

### **Assessment criteria for fraud investigations**

This criteria takes into account Home Office Circular **47/2004** 'Priorities for the Investigation of Fraud Cases'.

### **Cases considered for investigation.**

- The victim(s) are believed to be vulnerable. A person **may** be vulnerable by reason of age and/or their circumstances. Or, who suffers from mental or physical disabilities, illness, or other such special feature which renders them either permanently or temporarily unable to care or protect themselves against harm or exploitation.
- Businesses providing key services in difficult circumstances, or in distinct communities.
- Frauds having a significant impact on the victim(s). For example, a negligible loss to a large company could be catastrophic for a private individual or small business.
- The offence is believed to be part of a large linked series either partly or wholly within the Bedfordshire police area, Where the majority of lines of enquiry are in Bedfordshire.
- Strong positive lines of enquiry are immediately apparent.
- The offenders are part of an organised crime group and the activity reported would score 'high' on the harm matrix.
- There are clear opportunities to identify and restrain assets from the criminals with the aim of pursuing confiscation or forfeiture proceedings.

- The circumstances under investigation fall under the category of a critical incident, or the decision not to investigate could have a significantly detrimental effect on public confidence or satisfaction.
- Frauds giving rise to significant public concern, possibly highlighted by a high degree of press interest.
- Frauds involving substantial sums of money. (NB. Cases meeting the acceptance criteria of the Serious Fraud Office may be referred directly to them, either by the victim or the police).
- Frauds committed by, or knowingly facilitated by a person in a position of trust or professional advisers, e.g. lawyers, accountants, merchant bankers.
- Frauds likely to undermine confidence in leading UK institutions or otherwise undermine the economy.
- Frauds committed by members of boards or other senior managers.
- Frauds where law enforcement action could have a material deterrent effect.
- Frauds which indicate a risk of more substantial/extensive fraud occurring.
- Cases where the victim has devoted significant resources to fraud prevention or has been willing to participate in appropriate crime prevention partnerships or otherwise assist the police.
- Frauds which it has been agreed should be a current law enforcement priority.

#### **Cases unlikely to be investigated.**

- The investigation would require a disproportionate level of resource to bring the case to a conclusion and would adversely impact upon our ability to investigate other crime.
- Frauds where the likely eventual outcome, in terms of length of sentence and/or financial penalty, is not sufficient to justify the likely cost and effort of the investigation.
- The victim has pursued civil recourse and has subsequently turned to the police for a criminal investigation as a result of dissatisfaction with the civil remedy.
- Delays to the investigation will be caused by the location of key evidence elsewhere.
- Available resources will not permit an immediate and expeditious investigation.
- Victims have ignored guidelines that are designed to prevent them becoming victims of fraud, for example, online banking and auction sites.
- Frauds where the victim's conduct has contributed to the loss, in particular, where the police have previously given guidance or warnings to victims about fraud risks that have not been acted upon.

- Cases where the victim’s motive for making the complaint appears to be malicious, is primarily focused on recovering monies owed, or designed to distract attention from the complainant’s own involvement in the fraud. (Such cases might nevertheless merit investigation, particularly where there are other victims involved).
- Cases where victims are not prepared to co-operate fully with the investigation and prosecution, although we will always consider carefully how to assist victims and witnesses who have concerns about safety.
- Frauds more suitable for investigation by another enforcement or regulatory agency.
- Cases where another police force has decided not to investigate other than for geographical reasons.
- Frauds that have already been investigated by the police or another enforcement agency, or that have been the subject of regulatory proceedings, unless significant new evidence has come to light or the previous investigation had a narrow remit that did not address all the relevant issues.
- Cases where the existence of other proceedings might have a detrimental effect on a criminal investigation and subsequent prosecution.
- Frauds which took place a long time ago (probably more than 2 years), unless there are exceptional circumstances.
- The value of the loss does not warrant the investigative impact; and valued resources could be used on other priorities. Ie below £10,000 for business or £5,000 for individuals; unless above applies.

## 6. Associated Documents

- Home Office Circular [47/2004](#) ‘Priorities for the Investigation of Fraud Cases’.
- Fraud reporting advice
- College of Policing Fraud APP.

## 7. Consultation & Statutory Compliance

### 7.1 Consultation

Department – Internal	Comments
Force Crime Registrar	
Crime Recording Unit	
Public Protection Unit	
Signpost Victim Hub	
Divisional SCIT leadership	
Cyber Hub leadership	

Department - External	Comments
National Fraud Intelligence Bureau	

In most cases, the procedure will not need to be sent to JNCC and the above consultation will suffice. Final approval must come from your branch/divisional commander.

## 7.2 Statutory Compliance

### 7.2.1 Data Protection Act (1998)

The policy was assessed when originally published in March 2018. It is compliant with the Act.

### 7.2.2 Freedom of Information Act (2000)

The whole procedure can be released as there are no sensitive practices within the document.

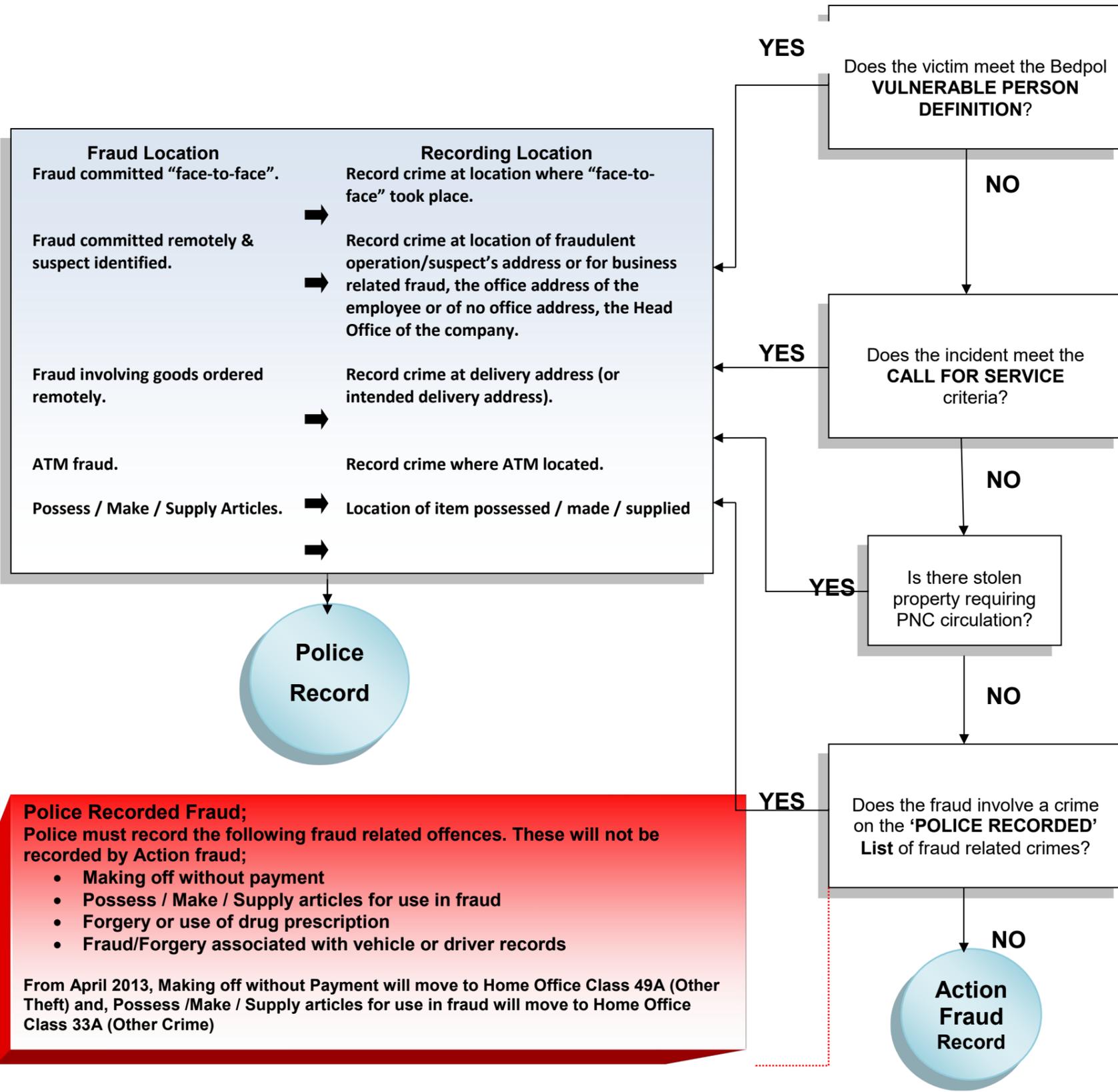
It has been agreed that this policy document will be made publicly available via the Bedfordshire police external website.

---

## 8. Appendices

Action Fraud guidance flowchart

# ACTION FRAUD GUIDANCE



**The Bedpol definition of a 'vulnerable person';**  
 A person may be vulnerable by reason of age and/or their circumstances, or, suffer from mental or physical disabilities, illness, or other such special feature which renders them either permanently or temporarily unable to care or protect themselves against harm or exploitation.

**'Call for service criteria', (covering all frauds), is met when;**

- Offences where offenders are arrested by Police or
- The offender 'is committing', has 'just committed or 'just attempted' fraud **and** has just made off prior to the call, or
- There is a known 'local' suspect. (The suspect has not been arrested at the scene nor just made off but police can or could locate a suspect with the details or CCTV images provided).

*Note\* Where monies have been withdrawn or credited to an account and a Data Protection Act (DPA) enquiry is required to establish the registered account holder's details (to determine their address and thus location of the offence) these frauds should be referred to Action Fraud. 'Local' means within force area.*

**Recording Location;**  
 Where the fraud or attempt fraud was 'face to face' and meets the call for service criteria, the fraud will be recorded and remain recorded on the 'face to face' location and will not be transferred to the suspects address even if established to be outside bedfordshire.  
 Where the fraud or attempt was 'face to face' but does not meet the call for service criteria, the crime will be recorded by Action Fraud.  
 Where the fraud was not 'face to face', with no identified suspect but was initially recorded by Bedfordshire due to a line of enquiry but during the investigation it is established that the suspect resides outside Bedfordshire the crime should be forwarded to Action Fraud for transfer.  
 Goods ordered remotely with a known delivery address will be recorded on the delivery address.

**Property Obtained By Fraud Requiring PNC Circulation;**  
 Action Fraud does not have access to the Police National Computer (PNC) and therefore the following action should be taken in relation to PNC registered items'(vehicle, plant, machinery etc.) when the property is outstanding:  
 'Call For Service' Police will be responsible for recording and retaining these crimes and also have the responsibility for PNC circulation.  
**No** 'Call For Service' Police will initially be responsible for recording these crimes whilst the stolen property is circulated on PNC. However, after circulation the crime should be forwarded by Bedfordshire Crime Desk to the NFIB for recording.

**Police Recorded Fraud;**  
 Police must record the following fraud related offences. These will not be recorded by Action fraud;

- Making off without payment
- Possess / Make / Supply articles for use in fraud
- Forgery or use of drug prescription
- Fraud/Forgery associated with vehicle or driver records

From April 2013, Making off without Payment will move to Home Office Class 49A (Other Theft) and, Possess /Make / Supply articles for use in fraud will move to Home Office Class 33A (Other Crime)

