Fraud Recording, Screening, Allocation and Investigation

Procedure

Greater Manchester Police

May 2020

Table of Contents

1. Introduction and Background

This document outlines the procedure for recording, screening, allocating, and investigating fraud offences. GMP decided to centralise the most serious fraud investigations and those investigations referred back to GMP by Action Fraud, other police forces or partner agencies, thus reducing the demand upon districts.

1.1 Aims

This procedure is intended to:

- Be victim focussed – ensuring compliance with the Victims Code of Practice (VCOP);
- Reassure colleagues they can make informed, sound, rationalised and value-based decisions using the National Decision Model;
- Influence crime allocation based on complexity and risk, not the type of crime;
- Provide a framework for staff, using the triage system, to use their knowledge and discretion to make the most effective and efficient decisions to achieve the best results for the victims of economic crime.
- Promote the use of a problem solving approach to target individuals and groups that cause threat, risk and harm. The triage framework should provide the team with confidence to make sound decisions on behalf of the organisation and our communities. This model set out is intended to assist the Economic Crime Unit (ECU) as well as GMP, together with our partners to do the right thing in line with the force strategy.
- Ensure investigations are conducted effectively, focusing on the risk posed to an individual or the wider public;
- Support supervisors in the management of crime;
- Provide a consistent approach: the Fraud Triage Team will process and score all fraud and cybercrime on behalf of the force, in conjunction with our partners and National Fraud Intelligence Bureau (NFIB).

GMP's Fraud Triage System is designed to reinforce the national fraud 'Four P' strategy in tackling fraud and cybercrime:

Pursue – Perpetrators of fraud will face the risk of prosecution, loss of assets and dismantling of their operations at every opportunity. The combined law enforcement response will attack the finances of organised crime, across regional, national and international borders. All statutory enforcement options available to police and our partners will be exploited to detect, investigate and disrupt criminality at the earliest possible stage, prosecuting those responsible and recovering assets.

Prevent – The police and partnership approach will be to deter people from engaging in fraud by raising awareness of its devastating impact, and showing that crime does not pay by marketing our success.

Protect – By working together in a cohesive partnership we aim to educate the public, and businesses, to prevent them becoming victims of fraud. Activities across the full spectrum of public and private sector partners will ensure alerts of fraud are rapidly communicated to potential victims. By understanding our emerging threats we will effectively drive targeted communications to help individuals protect themselves and reduce repeat victimisation.

Prepare - Given the rapid increase in fraud, both cyber enabled and otherwise, significant investment has been made to the future staffing and resourcing of fraud investigation. In conjunction with our partners we are ensuring an effective response.

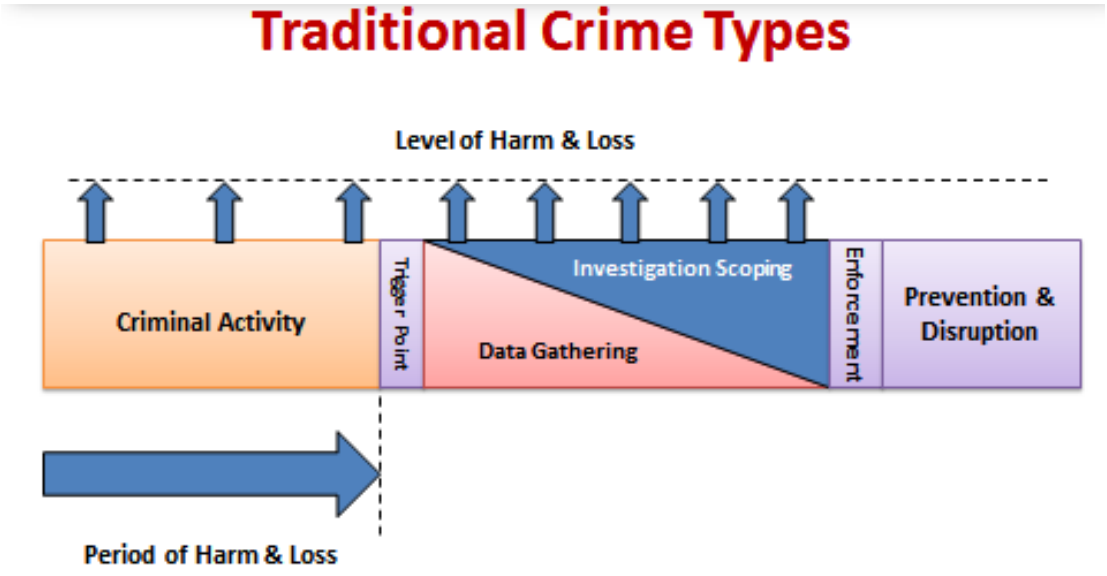
1.2 Background – Fraud Investigation Model

GMP have done much to professionalise the investigative process. This saw the use of a model of investigation, 'Core Investigative Doctrine', and is used extensively in the national detective program.

Although this core model was highly effective in most crime types, it did not take into account the unique nature of fraud. Hence the production of the Fraud Investigative Model (FIM).

When fraud is compared to traditional crime types there are some very significant differences. The traditional response is shown below.

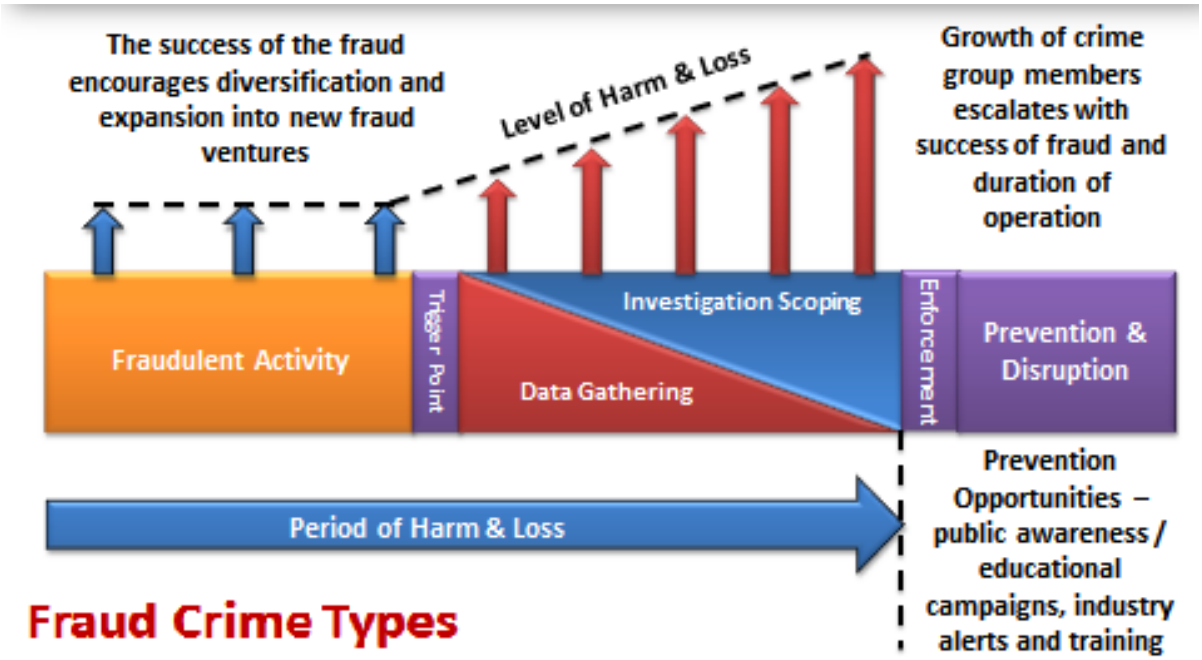
Figure 1. Traditional response to crime



As can be seen in the traditional response to non-fraud crime, the criminal activity occurs and the offence is subsequently reported. Following the report there is a period of data gathering and the investigation scoping those results in an enforcement action. Once the crime has been investigated, prevention and disruption opportunities may be considered. In many crime types this is an effective response, as the period of harm and loss is limited to the period of criminal activity and does not

increase over time. A useful example of this is an assault in a nightclub; the offence occurs, the victim reports the assault and the period of scoping commences to identify the offender. Meanwhile the offender has fled and is residing with an associate; no further offences are committed during this time.

Fraud is quite different, see **Figure 2. Fraud crime types, below.**

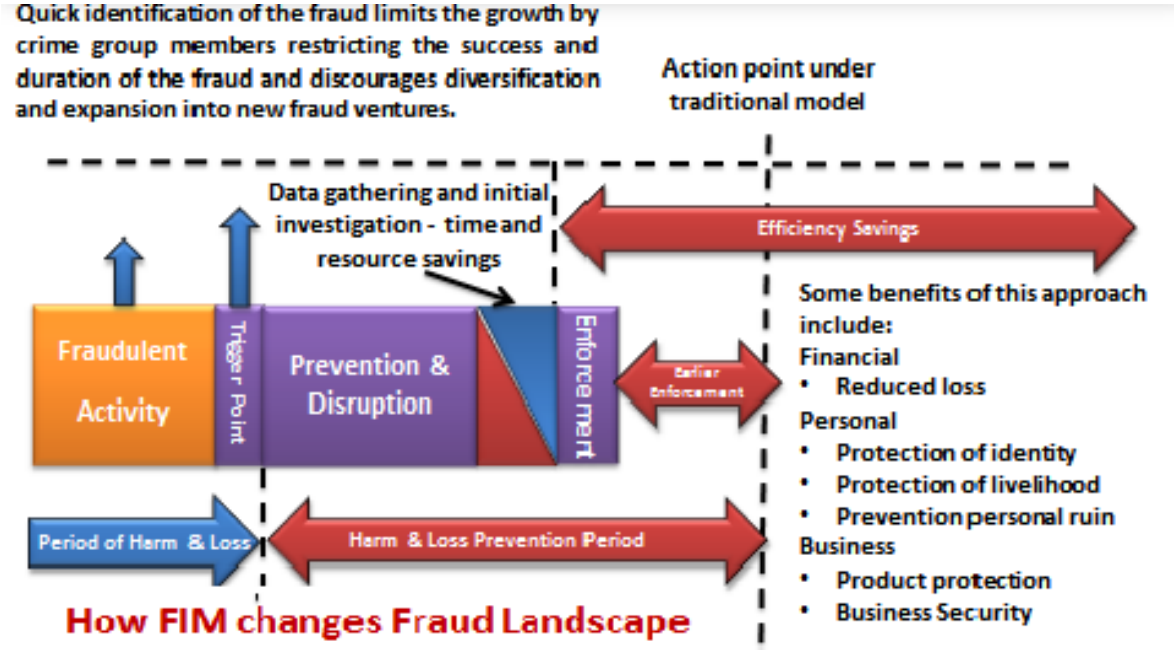


With fraud type of offences, the initial fraudulent activity takes place and the offence is reported. While the data gathering and investigative scoping takes place, due to the nature of the fraudster, further offences are committed. This increases both the level and period of harm: in many cases if left unchecked the fraudster will develop new types and styles of fraud as well as enhance his skills at this type of fraud. If left unchecked the harm caused by the fraudster is perpetually increased.

There is, therefore a need to limit the periods of harm and loss by stopping the fraudster at the earliest opportunity. As such, following the instigation of the case, emphasis is placed upon opportunities for early disruption and prevention.

As per the diagram below, the effective use of the FIM will reduce the potential period of harm caused by the fraudster. Subsequently the loss caused is significantly mitigated by reducing the enablers and vulnerabilities that the fraudster uses to perpetrate their crimes.

Figure 3. How the FIM changes the fraud landscape.



2. Scope

This procedure is aimed at staff who work within the following areas:

- Economic Crime Section
- Cecas and Scambusters
- Districts
- Crime Recording Unit
- Operational Communications Branch.

3. Roles & Responsibilities

3.1 Call Takers, Operational Communications Branch

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. 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 an incident on Control Works and a police officer should be allocated to deal with the report. See Fraud – Calls for Service Guidance shown at Appendix 1.

3.2 Initial Investigating Officer, District

The initial investigating officer and reviewers of the crime, must consider the following key points throughout:

Four Fraud Prevention Questions in the Fraud Investigation Model

- What were the principle enablers that allowed this fraud to be perpetrated?
- Who else could be at risk from this or a similar fraud?
- What could have been done to remove or reduce the risk from this fraud?
- How can the lessons learnt be used to prevent others from becoming victims of a similar fraud?

If you are the first responder dealing with a report of a fraud crime on a district, 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 close circuit television (CCTV). **Initial investigations should comply with the PIP 1 write-up standard.**
    - 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 Economic Crime Section, Serious Crime Division.
    - Scan and email a copy of all statements and supporting documentation, with the crime reference number, to the economic.crimedesk@gmp.pnn.police.uk, or send by internal mail to the Fraud Triage Desk. This may not be possible in more complex cases. Please note that statements and some supporting documents when completed are classified as 'Official Sensitive' under the Government Security Classification but may be forwarded by internal mail **in a sealed envelope** which should not indicate any classification. The use of transit envelopes should be avoided.
    - 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. Greater Manchester Police will pass information via the Crime Recording Unit to Action Fraud on the victim's behalf.

3.3 Fraud Triage Researchers

On receipt of an action to obtain the National Fraud Recorded Crime Number (NFRC) through the crime management system, fraud triage researchers are to log onto the 'Expert Recording Tool' and conduct actions to obtain the NFRC number.

On receipt of an action fraud referral, fraud triage researchers are to create a crime report on iOPS and cross reference all relevant material on the crime report. It must be remembered that only one victim is to be shown on the crime, with the remainder being added as witnesses. Please note that businesses are not to be recorded as victims.

The NFRC number is to be stored under the header "OBJECTS" on the iOPS system.

Fraud triage researchers are also to create a Cyclops reference in each case. This is important for the storage of all documents passed or obtained.

Research in each case is to be conducted in line with the internal Economic Crime research guidance.

On a daily basis fraud triage researchers are to log into the NFIB vault and review this system for new allocations to GMP.

On receipt of instructions from the Cyber Crime sergeant, crimes are to be created where instructed and allocated to detective sergeants Cyber Crime for actioning and dissemination. (In these cases, no research is required).

On receipt of correspondence and referrals from Police Scotland treat as a NFIB referral and create a crime storing documents on Cyclops.

3.4 Crime Recording Unit

You should send all relevant fraud cases, where possible, to the evaluators on the Fraud Triage Desk, Serious Crime Division.

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' and the flagging marker is complete on the crime. Flags should be ticked on iOPS; these can be found in the initial details section of the 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 GMP report.

3.5 Fraud Triage Evaluators, Serious Crime Division

You should evaluate all fraud cases and fraud related correspondence in accordance with this procedure.

All reports of serious fraud, screened in and accepted for secondary investigation, will be investigated by Fraud Investigation Teams (FITs) or Cyber Crime Support

Team within Serious Crime Division, or other GMP resource, as agreed by the Economic Crime Section management.

Any allegation of fraud that is considered as complex and/or is clearly being committed by an Organised Crime Group (OCG) will be assessed the detective sergeant, Intelligence Team. All fraud of this type screened in for secondary investigation, will be investigated by the Fraud Investigation Team, Cyber Crime Support Team, Intelligence Team or other GMP resource as agreed by the Economic Crime, Section management.

You should ensure that all fraud reports are recorded at the National Fraud Intelligence Bureau.

3.6 Detective Sergeant Fraud Triage Desk

You are responsible for the consistent approach to the screening of crimes for secondary investigation in line the National Decision Model and those decisions are fully rationalised and documented in line with this procedure and National Crime Recording Standards. In addition, screening decisions will be made based on threat, harm, opportunity, risk and vulnerability in line with the factors outlined within the Crime Management Policy and Procedure.

4. Terms and Definitions

4.1 Terms

Action Fraud – National Fraud Reporting Centre

Action Fraud and the National Fraud Intelligence Bureau – are governmental organisations tasked with the recording of all fraud reported in England and Wales.

Cyclops – is an investigative database, used by the Economic Crime Unit that additionally records and stores documentation received in an electronic format.

Huddle - Is an ECU meeting to establish if a raised crime is suitable for No further Action, initial scoping or adoption for an investigation.

4.2 Acronyms

CCTV – Closed-circuit television

CECAS – Cyber and Economic Crime Awareness Service

CPT – Crime Progression Teams

ECU – Economic Crime Unit

FIM – Fraud Investigation Model

FIT – Fraud Investigation Team

HOT – Harm, Opportunity, Threat

iOPS – Integrated Operational Policing System

MO – Modus operandi

NDM – National Decision Making

NECVCU - National Economic Crime Victim Care Unit, within Action Fraud.

NFA – No further action

NFIB – National Fraud Intelligence Bureau

NFRC – National Fraud Recorded Crime Number

OCG – Organised Crime Group

OCCU – Organised Crime Co-ordination Unit

PNC – Police National Computer

VCOP – Victims code of practice

5. Procedure

5.1 Reporting a fraud – Action Fraud Criteria

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:

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

5.2 Calls for Service

Calls for service is explained at Section 3.1, and also in Appendix 1. This includes circumstances where the police would be expected to attend an incident and record a report of crime as opposed to referring the victim to Action Fraud for reporting purposes. The criteria for a police report of fraud is where:

- There is an identified vulnerable person in line with GMP's description
- 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 stolen property requiring PNC circulation.

5.3 Deciding Whether to Investigate (Crime Screening)

Decisions by supervisors on whether to further investigate should be made using the GMP's Cyber and Economic Crime model integrated with the National Decision Model (NDM), found at Appendix 2, and in particular:

- The principles set out in Section 1.1, above;
- Making decisions which are reasonable and justified; and
- Making decisions at all times with consideration of what the public would reasonably think.
- Screening decisions will be made based on threat, harm, opportunity, risk and vulnerability in line with the factors outlined on the Crime Management Policy and Procedure.

Decisions and rationale for whether or not to investigate are recorded on the crime log within iOPS.

Due to the unique and varied circumstances around each fraud case reported, the Cyber and Economic Crime NDM contains guidelines for consideration by the investigator. This is not exhaustive or prescriptive, however it is recommended that consideration is given to which category a case falls into to assist decision making. Where a decision is made not to investigate, the rational **must** be included in the crime report update.

5.4 Being Victim Focused - Understanding Victim Vulnerability and Impact

Listed below are considerations the evaluator is to take into account when trying to understand the vulnerability issues around a victim's status:

- The victim/location or offender is a repeat;
- The victim is vulnerable;
- The crime may be hate related;
- Harm, Opportunity, Threat (HOT) crimes in accordance with the established Force definition;
- Significant public concern or media interest;
- The value of the stolen/damaged property and victim impact (high or low);
- The victim has pursued civil recourse and has subsequently turned to the police to commence a criminal investigation, as a result of dissatisfaction with the civil remedy;
- The victim(s) appears to have reported the crime for administrative reasons, e.g. to obtain a crime reference number for an insurance claim, and has no expectations regarding the outcome of an investigation;
- There are doubts over the veracity of the report but no credible evidence to the contrary to 'no crime';
- Victim(s) appears to have wilfully ignored guidance to prevent them becoming a victim of crime;
- The victim's motive for making the complaint appears to be malicious or is designed to distract attention from their own involvement;
- Victims are not prepared to fully cooperate with the investigation and prosecution (unless operating under duress).
- The victim has no expectations the crime will be investigated;
- Victims of fraud are likely to become further victims unless protection measures are in place;
- Cases where the victim has devoted significant resources to fraud prevention or has been willing to participate in appropriate crime prevention partnerships.

These factors are information or opinion about the victim and would be disclosable to them if the crime report was requested under subject access. Officers should be aware and ensure that the rationale is appropriately and professionally worded.

5.5 Protection of the Public - Understanding Offender Threat/Harm and Impact

Below is a list of considerations the evaluator is to take into account when trying to understand the **Threat/Harm and Impact around an offenders status.**

- Offence motivated by **discrimination** and/or **hate;**
- Community impact;
- Serious offence;
- Part of a linked or emerging series;
- Priority Offender;
- Risk and capability of the offender;
- Offenders/offence linked to organised crime;
- Targeting of vulnerable victims;
- Use of a weapon of threat of violence;

- Suspect is, or was, at the time of the offence suffering from significant mental or physical ill health.
- There are clear opportunities to identify and restrain/freeze assets from offenders or disrupt their activity.
- Circumstances that may cause an investigation to fall under the heading of a critical incident, or frauds giving rise to significant public concern.
- Frauds committed by, or knowingly facilitated by, professional advisers, e.g. lawyers, accountants, merchant bankers.
- Cases more suitable for investigation by another enforcement or regulatory agency.

5.6 Making the Most Effective Use of GMP Resources

The list below are the points the evaluator must consider when deciding on the police response.

- The investigation would require a disproportionate level of resource to bring the case to conclusion and would adversely impact upon our ability to investigate other crime;
- Another police force or law enforcement agency has decided not to investigate other than for geographical reasons;
- The crime is a historic crime and there are no exceptional circumstances.
- Problem solving opportunities to reduce demand.

The above lists are for guidance only and are not, and cannot be, exhaustive. They are to assist the understanding of the process.

To ensure the standards of evaluation and especially write up, when assessing fraud crimes it is essential to:

- Follow our principles (see Section 1.1);
- Use policing experience and common sense; and
- Make reasonable and justifiable decisions which would withstand public scrutiny.

5.7 Key Decisions

In line with the PIP 1 Crime Management Standard, the basis of screening rationale should be Threat, Harm, Opportunity and Risk**.**

The key decision-making factors include: -

- Seriousness and Vulnerability
- Solvability
- Victims Wishes
- Resource Availability

It is essential that whilst reviewing a report of crime, or correspondence etc. we consider the following points:

- Read the modus operandi (MO); is there an actual offence or civil dispute or no crime?
- Is the crime HOT, based on the circumstances? If not REMOVE flag.
- Gain a full understanding of the case so that the following areas can be addressed. (In line with the ECU Scoring Matrix)
    - Seriousness of the offence, (Based on offence type)
    - Complexity;
        - Evidential assessment/solvability
        - Geographical scale
        - Volume of victims/offenders
        - Resource logistics (where do the enquiries sit, locally, national or internationally)
    - Threat posed by or to;
        - Victim
        - Offender
    - Harm caused/impact of offence to, either:
        - Individual or
        - Business
    - Opportunities, to
        - Prevent/disrupt
        - Financial recovery or targeting.
    - Is there anything else that may influence a decision to screen in or out?

- What if any further research is required at this time and where does that sit?

By applying this consistent approach, we would have an understanding of the investigation, and whether we would then need to:

1. Request further information, conduct further research, and speak with the victim.
2. Screen the matter out for no further action (NFA).
3. Request scoping of an enquiry.
4. Screen in for adoption by the FIT syndicates, via the Triage Sergeant and Crime Management and Review Process.

5.8 Initial Write Up

When conducting a write up for screening we need to comply with the criteria shown below, namely:

- Outline what has happened.
- Outline if any HOT principled action is required.
- An update of the points outlined in the above page, and if specifically, any areas are identified as high risk.

- Recommendations for screening in/screening out and any actions that are required before a decision is further made if that is the case.
- Highlight areas of opportunity to Prevent/Disrupt/Pursue/Protect
- Pre-order checks to be conducted where we have an open account and there is a loss to the victim of over (Figure set by ECU based on current capacity).
- Mandate fraud cases should be given priority by evaluators, due to the amount lost within these type of offences and the fast time actions that may be available within this type of case.

The ECU Triage evaluator has a uniquely different role to any other force (Crime Progression Team) evaluator. This role includes in part researcher, primary investigator and evaluator.

Many of the crimes that are reviewed in this area are positive lines. They can show substantial losses or a number of victims. However it must always be remembered that at this time, we have a duty to provide resources to the most vulnerable or at risk, or those causing harm in our communities. We have limited resources and a centralised responsibility for serious fraud. At times there will be difficult decisions to be made, decisions that elsewhere as an investigator you would expect to take on. This is simply not possible at this time and we must prioritise our investigations. It is therefore essential that we try and remain consistent in our decision-making progress.

At this time scores (set by ECU Senior Leadership Team) are to be forwarded to the detective sergeants for consideration of presentation at the Huddle for potential adoption by the FIT. There will be a review monthly at the crime management meeting as to the movement of the referral criteria.

Albeit we may not take on an investigation, there will still be opportunities to protect the victim, prevent this happening again, and target the offender via disruption activities.

5.9 Scoping

There will be crimes where a decision cannot be made as to whether a FIT syndicate would be allocated a case for adoption/further investigation from the outset. In complex cases these can be allocated, via the Crime Management Process, for allocation to a FIT syndicate to make these necessary enquiries. By allocating to a FIT syndicate, should the case eventually be adopted, an investigator would have a full understanding of the case.

5.10 Allocation and 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 originating from Action Fraud, other forces or partners will be assessed by the Fraud Triage Desk, Serious Crime Division. Calls for service will be assessed by the respective districts. Support for district crime progression teams (CPTs) is available in line with Appendix 1.

In cases where the crime is screened in for further investigation, the crime will be allocated to the Fraud Investigation Team or the Cyber Crime Support Team, or other GMP resource as agreed by the Economic Crime Section management.
Exceptions to this will include:

- Offences of making off without payment and other minor fraud offences detected at source which will continue to be dealt with directly by districts.

- Frauds reported as a call for service where there is a local district based vulnerability that needs to be addressed as a primary concern, such as abuse of positions in care homes or family, control settings.

All complex fraud allegations will be assessed by the Economic Crime Section tasking and coordinating group and where the crime is screened in will be investigated by the Fraud Investigation Teams, Cyber Crime Support Team or the Intelligence Team, Serious Crime Division or other GMP resource as agreed by the Economic Crime Section management.

5.11 Finalising crimes

All recorded crimes must have the correct outcome appended at the point of finalisation. When an investigation has come to its conclusion the OIC should submit the crime to their supervisor to endorse with a disposal summary. The disposal summary should document the rationale for the chosen outcome for each named suspect. The supervisor should then finalise the crime.

Evaluators have the authority to finalise fraud crimes through the triage process, however the detective sergeant is responsible to ensure that all necessary parts of the crime report are complete, a suitable victim letter is sent (in line with recognised iOPS Template Fraud letters) and that there is a clear and rationale justification outlined on the crime report. This will be monitored via a dip sampling process organised within the ECU.

5.12 Crime Reclassification/Cancellation

Crime classification is set at the time of initial recording. If further information comes to light after the crime has been recorded, it may be reclassified.

The request to reclassify a crime must be submitted to the detective sergeants Fraud Triage Desk for initial review and once approved, referred to the Crime Audit Team with documented rationale as to the reason for reclassification, together with the new crime classification requested. The Crime Audit Team will then administer the reclassification.

The request to cancel a crime must be submitted to the detective sergeants Fraud Triage Desk for initial review and once approved, referred to the Crime Audit Team with documented rationale as to the reason for cancellation. The Crime Audit Team will then administer the cancellation.

5.13 Appeals Process

The victim or person reporting may be dissatisfied with the decision not to further investigate the crime.

A nominated person senior to the decision maker should act as the appeals manager. This does not affect the victim's right to make a formal complaint via the appropriate channels, but is intended to provide an alternative route to early resolution.

The appeals manager should use the NDM taking into account the scoring matrix to assess whether the decision maker has appropriately considered and communicated the above factors to the victim or person reporting. They must speak to the decision maker to make this assessment and should consult with the district Victims Services Coordinator.

Where the victim remains dissatisfied the appeals manager should escalate to the Crime Manager who will make the final determination.

5.14 Cyber and Economic Crime Awareness Service and Scambusters

The Cyber and Economic Crime Awareness Service (CECAS) was created in 2017 due to the large numbers of fraud and cybercrime victims being recorded nationally, but not locally, so were hidden from usual crime recording standards. The service works closely with Action Fraud, National Economic Crime Victim Care Unit (NEVCVU), the banking sector and third-party support agencies to provide advice and support to vulnerable victims of fraud as well as those identified as potential future victims. So far, over 2000 victims have been supported through CECAS, with only two CECAS victims being secondary victims of fraud.

Please do not delete any actions for our CECAS team on iOPS.

Our CECAS can be contacted on the following email- FraudStrive@gmp.police.uk

Scambusters

Over the past 12 months there have been significant changes in the way the Economic and Cybercrime Service has been channelling resources into prevention, safeguarding and community engagement across the whole of Greater Manchester. We have recruited our 'Scambuster' central team of volunteers, with a view to this going force-wide moving forward.

The CECAS and volunteers contact victims every day by telephone and give out fraud prevention material. They also organise community events to spread the prevention message.

The Scambuster's phone number is 0161 856 4120.

6. Associated Documents

- Crime Standards Policy and Procedure

7. Statutory Compliance

7.1 Equality Act (2010)

In producing this document, due regard has been given to the General Equality Duty. The procedure emphasises the need to be victim-focused and advises supervisors to take the victim's specific needs into account when deciding whether to further investigate a crime, for example if the victim is vulnerable (which may be due to their protected characteristic, e.g. age/disability). Additionally, the procedure emphasises the responsibility on the supervisor to ensure the most appropriate resource is allocated to the crime in order to conduct the investigation in a timely manner, whilst delivering the best level of service. The management of crime references the need to adhere to HOCR and NCRS, thus promoting ethical crime recording for all victims of crime.

This procedure promotes consistency in service standards which will ensure that victims receive the same high level of service wherever they live in Greater Manchester, and regardless of their age, religion, or sexual orientation etc.

7.2 The General Data Protection Regulation (GDPR) and Data Protection Act (2018)

Greater Manchester Police has a duty to ensure, so far as is possible, that all staff comply with the provisions of the GDPR and the Data Protection Act 2018, particularly relating to their access to, and dissemination of, a wide variety of personal information and intelligence.

The Information Compliance & Records Management Unit has assessed this procedure; the purpose of this procedure is compliant with the Data Protection Act 2018 and the processing and sharing of information outlined in this procedure is in conjunction to a clear lawful basis (law enforcement processing – Part 3 DPA 2018) which is detailed within the policy.

7.3 Freedom of Information Act (2000)

This procedure is available for the public and can be used for Freedom of Information requests.

8. Appendices

Appendix 1 – Fraud - Calls for Service Guidance

Appendix 2 – GMP's Cyber and Economic Crime Decision Model