



Fraud Allocation and Investigation

Owning Department:	Head of Safeguarding & Investigations Command / Head of Crime / ACC Operations		
Chief Officer Lead for Fraud	T/Assistant Chief Constable		
Senior Strategic Fraud Lead	T/D/C/Superintendent		
Operational Fraud Lead / Dept SPOC	DCI Investigations		
Dissemination/Triage SPOC for Fraud	Athena Investigations Hub Supervisor		
Communications Lead	Senior News Officer		
Risk Rating:	Low	Legal Sign Off: Date:	10.01.2020

Approved by

JNCC:	11.12.2019		
Published Date:	16.12.2019	Review Date:	16.12.2023

Index

1. Summary of changes	3
2. Introduction.....	3
3. Aims	5
4. Statement of Policy	5
5. Roles and Responsibilities	5
Action Fraud (AF)	5
The National Fraud Intelligence Bureau (NFIB).....	6
The City of London Police	6
National Crime Agency (NCA).....	6
Regional Fraud Teams (RFTs).....	6
Force-level economic crime and fraud capability.....	6
Government Departments	6
Complaint of Fraud Relating to Local Authorities	8
6. Action Fraud – Reporting, Assessment and Investigation Process (Appendix A)	8
7. Norfolk Constabulary – Reporting, Assessment and Investigation Process (Appendices B & C)	9
8. Officer Response to ‘Call for Service’	10
9. Crime Evaluation (IMU)	11
10. Fraud Investigation Model (FIM).....	11
11. Escalation process to ERSOU or reallocation within NC	12
12. Established Preventative Measures	13
Operation Bodyguard	13
Banking Protocol	14
13. Resources	15
ERSOU	15
RECU	16
RART	16
14. IMU Reporting Returns to NFIB.....	17

Please Note: Appendices are referred to throughout this policy, however due to security classification purposes, these have been redacted from this version

Security Classification:	OFFICIAL
---------------------------------	----------

Legal Basis

Legislation specific to the subject of this policy document

Section	Act (title and year)
	Fraud Act 2006
	Theft Act 1968
	Criminal Procedure and Investigations Act 1996 (CPIA)

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health and Safety at Work etc. Act 1974 and associated Regulations
General Data Protection Regulation (GDPR) and Data Protection Act 2018
Freedom Of Information Act 2000
The Civil Contingencies Act 2004

Other documentation which you must check this document against

Document
College of Policing – Code of Ethics
Norfolk and Suffolk Constabularies’ Standards of Professional Behaviour
College of Policing – Authorised Professional Practice
Investigation of Fraud and Economic Crime (Blackstone’s Practical Policing, Michael J Betts)
Fraud: Time to Choose. An inspection of the police response to fraud. HMICFRS

1. Summary of changes

- 1.1 This is a new policy that relates to Norfolk Constabulary’s investigation of fraud.
- 1.2 This policy does not replace previous policies.

2. Introduction

- 2.1 Fraud and economic crime represent significant threats to communities across the United Kingdom (UK), particularly to businesses and the vulnerable. It is recognised that the volume of fraud impacting on the UK is growing in complexity and diversity.
- 2.2 Fraud has been globalised and the reach of the fraudster has increased through the use of new technologies, enabling traditional crime to be committed in new ways through the use of computers, computer networks or other forms of information communications technology.

Security Classification:	OFFICIAL	Version:	1.1
---------------------------------	----------	-----------------	-----

Security Classification:	OFFICIAL
---------------------------------	----------

- 2.3 In 2016, the estimated loss attributable to fraud across the UK was £193 billion (Annual Fraud Indicator 2016, Experian, PKF Littlejohn LLP (PKF) and Portsmouth University, 2016).
- 2.4 The estimation of loss to businesses and organisations around the world is an average of 5.6 per cent of their annual expenditure.
- 2.5 The volume of fraud impacting on Norfolk is growing in line with the national picture. Those who commit fraud often exploit and profit from misplaced trust and act to the detriment of public through the serious harm they cause.
- 2.6 Norfolk's Fraud Profile (April – September 2018) is in line with national trends, it shows a 12% rise in fraud (11% National), 16% of all victims are identified as vulnerable (3 in every 20), phones are the most common fraud enabler (40% Norfolk, 33% National), most reported cyber-dependent crime is Hacking – Social Media and Emails.
- 2.7 Norfolk's Fraud Profile identifies similar quantities of loss between businesses and individuals.
- 2.8 Fraud and economic crime represent significant challenge to enforcement organisations and investigators. Fraud is often made more complex by the range of enablers and mechanisms to conceal the movement of money and true nature of the fraud.
- 2.9 Key challenges are assessed as relating to officer capability (training and knowledge), effective joint data opportunities (rich picture) and demand versus capacity.
- 2.10 This policy recognises the scale of fraud related offences, significant loss and impact to businesses and individuals, a proportion very vulnerable. This policy seeks to ensure that Norfolk Constabulary prioritises fraud investigations appropriately and supports national priorities.
- 2.11 This policy recognises Norfolk Constabulary's part in a wider established network of enforcement agencies and partners in contributing to the effective response to fraud.
- 2.12 This document sets out roles and responsibilities, reporting structures, assessment process, the Fraud Investigation Model (FIM), established preventative mechanisms and resources. It also seeks to deal with internal and external escalation processes.
- 2.13 It is every officer's responsibility to deal with fraud offences in accordance with the procedures laid down in this document.

Security Classification:	OFFICIAL	Version:	1.1
---------------------------------	----------	-----------------	-----

3. Aims

- 3.1 To make clear the national structure in place to deal effectively with fraud investigation and Norfolk Constabulary's part in it.
- 3.2 To define roles and responsibilities of City of London Police, the National Crime Agency, regional crime units and police forces.
- 3.3 To provide clear ownership and direction for Norfolk Constabulary staff in understanding reporting structures, lines of responsibility and escalation processes.
- 3.4 To define Norfolk Constabulary's response to investigation of fraud related offences.
- 3.5 To outline effective structures that have already been put in place within Norfolk Constabulary with partner agencies.

4. Statement of Policy

- 4.1 This policy is supported by Norfolk Constabulary's current vision and values.
- 4.2 Norfolk Constabulary will ensure that the policing response to reports is in line with national guidance relating to action fraud reporting or local ownership.
- 4.3 Norfolk Constabulary has a duty to protect vulnerable persons from crime and will ensure that the necessary mechanisms are in place to safeguard the vulnerable from fraud.

5. Roles and Responsibilities

- 5.1 There are currently local, regional and national structures in place for fraud related matters.
- 5.2 It is recognised that there should be a level of collaboration and partnership working across public and private sectors to combat economic and fraud criminality.

Action Fraud (AF)

- 5.3 Action Fraud is the UK's national reporting centre for fraud and cyber crime where instances of fraud, cyber crime and scams should be reported. It covers England, Wales and Northern Ireland.
- 5.4 Action Fraud provide a centralised point of contact for information about fraud and financially motivated internet crime.
- 5.5 The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB).

The National Fraud Intelligence Bureau (NFIB)

- 5.6 The NFIB are responsible for assessment of the reports and to ensure that fraud reports reach the right places. This involves processing and analysing fraud data to provide actionable intelligence and emerging issues and trends for disruption and prevention. NFIB develop and allocate crime packages to facilitate local, regional and national police functions and law enforcement agencies.
- 5.7 The Home Office requires NFIB via Action Fraud to record fraud for statistical purposes. The Home Office will obtain data on fraud levels for NFIB Recorded Fraud and Cyber offences from the NFIB. This will consist of the national total level of NFIB recorded fraud / cybercrime, demand on police by Force area and result of that demand (i.e. outcomes).

The City of London Police

- 5.8 The City of London Police are the national lead force for economic crime. The National lead force (NLF) was created to provide specialist support and guidance regarding fraud education and investigation to police forces, other law enforcement agencies and industry. They are also responsible for carrying out investigations for those frauds that cause the greatest harm.

National Crime Agency (NCA)

- 5.9 The NCA targets criminals and groups posing the biggest risks to the UK by conducting its own operations, providing operational and specialist support to partner agencies and ensuring UK law enforcement makes best use of collective resources.

Regional Fraud Teams (RFTs)

- 5.10 RFTs are embedded within the existing national Regional Organised Crime Unit (ROCU). There are nine ROCUs across the UK supporting the 43 police forces. RFTs initiate proactive and reactive investigations.

Force-level economic crime and fraud capability

- 5.11 These exist in a number of police forces. Norfolk does not currently have such a unit, although the joint-force Cyber Investigations Team (see 13.17 below) does pick up complex frauds which are cyber-dependent. As such fraud investigations are primarily dealt with by Criminal Investigation Departments (CIDs), Adult Abuse Unit (AAU), dedicated units supporting front line investigations or front line officers.

Government Departments

- 5.12 There are a number of government departments which also have a statutory responsibility to investigate certain fraud types. They include:

Security Classification:	OFFICIAL	Version:	1.1
---------------------------------	----------	-----------------	-----

- [Department for Work and Pensions \(DWP\)](#)
DWP investigates benefit frauds.
- [Single Fraud Investigation Service \(SFIS\)](#)
SFIS works with DWP, Her Majesty's Revenue and Customs (HMRC) and local authorities to investigate and prosecute welfare fraud and tax credit fraud.
- [Her Majesty's Revenue and Customs \(HMRC\)](#)
HMRC is responsible for investigating serious organised fiscal crime and suspected tax fraud.
- [Serious Fraud Office \(SFO\)](#)
SFO is an independent government department responsible for protecting society by investigating those who commit serious or complex fraud, bribery and corruption and pursuing them for proceeds of their crime.
- [Charity Commission](#)
This raises awareness of fraud among trustees and wider public, they provide alerts and warnings to raise awareness of specific frauds and risks and publish wider lessons learnt.
- [Insolvency Service](#)
This has responsibility for administering and investigating companies that have gone into compulsory liquidation or received bankruptcy or debt relief orders. They also investigate allegations of misconduct in live companies.
- [NHS Counter Fraud Authority](#) (previously known as NHS Protect)
This is part of the NHS Business Service Authority. It investigates fraud, bribery, corruption and other unlawful actions within the National Health Service.
- [UK Intellectual Property Office \(IPO\)](#)
Investigate intellectual property (IP) offences. IP relates to copyright, design, patent or an idea that takes a tangible form.
- [Her Majesty's Passport Office \(HMPO\)](#)
HMPO investigates fraudulent passport applications and offers passport validation service.
- [Cabinet Office Fraud, Error, Debt and Grant Function](#)
This is a service responsible for setting government standards for fraud and error and providing strategic leadership on these matters.

Complaint of Fraud Relating to Local Authorities

- 5.13 All public bodies including local authorities (such as Local Councils, Police and Crime Commissioners) are monitored and scrutinised by External Auditors appointed by the Public Sector Audit Appointments. External audit was privatised by the government in 2015 and passed the responsibility to accountancy firms appointed under the frameworks by the Public Sector Audit Appointments (albeit with responsibilities to report back to government). The relevant external auditor can be identified by searching [here](#).
- 5.14 The External Auditors will report to the Ministry of Housing, Communities and Local Government (MHCLG) – Efficiency and Accountability unit who will appoint ‘Commissioners’ who step in to take over the council, MHCLG or the appointed Commissioners then report criminal issues to the police or the National Investigation Service (NATIS).
- 5.15 Further guidance can be obtained by contacting the National Investigation Service (NATIS) on: Tel. 03000 999111.

6. Action Fraud – Reporting, Assessment and Investigation Process (Appendix A)

- 6.1 This section deals with the reporting, assessment and allocation of investigation process at Action Fraud level.
- 6.2 It does not deal with local reports made to local police forces.
- 6.3 Following a crime report being made to Action Fraud, the NFIB are required to assess that report.
- 6.4 This will focus on two primary parts, the first a victim assessment, the second an investigation assessment.
- 6.5 The victim assessment will involve assessing whether or not the victim is identified as vulnerable or in need of additional support. If identified as vulnerable, intelligence will be passed to the local police force to consider an investigation or for victim care.
- 6.6 The investigation assessment will consider three main criteria: i) if there are lines of inquiry linked to the report which are likely to identify a suspect, ii) are there suspect details linked to report, e.g. bank account, website, phone numbers and similar; and iii) is there information in the report that would be helpful to partner agency here or police force overseas.
- 6.7 If any of the above criteria are fulfilled the intelligence/investigation will be passed to either a local police force or partner agency (or overseas agency) to consider an investigation or for victim care.

6.8 Each report is retained and continually compared against new information through NFIB assessment.

6.9 As of 2nd December 2019 Police Scotland will no longer participate in using Action Fraud, any report of fraud relating directly to Scotland should be dealt with in accordance with the guidance included at [Appendix E](#).

7. Norfolk Constabulary – Reporting, Assessment and Investigation Process (Appendices B & C)

7.1 The ‘demand on police’ is to investigate offences that meet the ‘call for service’ criteria and offences passed to the Force by the NFIB for law enforcement.

7.2 Where victims contact the police to report a fraud, the police may, unless a police ‘call for service’ exists, advise the victim that they can report the fraud to Action Fraud directly via the contact centre or on-line reporting tool. If this advice is taken, then there is no need for police to record a crime or information report.

7.3 ‘Calls for Service’ relate to reports where:

- Offenders are arrested by police; or
- There is a call for service to the police and the offender is committing or has recently committed at the time of the call for service; or
- There is a local suspect.

NB. Where 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, a police record should be made. This does not preclude dissemination to AF following consideration of safeguarding if other ‘call for service’ criteria is/are not met.

If a crime meets the service criteria or if the victim is identified as requiring safeguarding, the Constabulary will initiate the investigation. These will be undertaken by uniform / detective resources depending on the nature of the offence and vulnerability. This will include referrals to Crime Prevention and partnership agencies for support and to prevent re-victimisation.

The nature and level of assistance is often linked to the vulnerability of the victim and/or whether they have been repeatedly targeted. The Multi-Agency Safeguarding Hub (MASH) will facilitate contact with support services (e.g. Adult Social Care) if the vulnerability is linked to a need for support managing prevention surveys, advice to relative/carers and liaison with the financial institutions to prevent further victimisation.

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

- Police can or could locate the suspect with the details provided;

- Have sufficient details to apprehend an offender.

'Local' has its everyday meaning and has been used to ensure that, as with any other crime, where there are local viable investigative leads, police should consider the crime for investigation.

Where this is not the case and the crime needs to be transferred, the crime should be passed to the NFIB or referred to Action Fraud if appropriate.

7.4 **Police Recorded Fraud** relates to fraud that must be recorded by the police and will not be recorded by Action Fraud, the offences are:

- 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.

7.5 Police Officers and Police Staff are responsible for:

- Considering if the person reporting should be referred to their bank / financial institution or Action Fraud;
- Creating a Storm log and tasking for resources to be deployed where a report meets the Call for Service criteria;
- Creating a Storm log and deploying resources where the offence meets the 'call for service' or vulnerability criteria (section 7.3):
 - 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.

NB. Action Fraud will not deal with the above and these cases should not be referred to them.

- Referring frauds where a motor vehicle or plant equipment has been stolen to Action Fraud after a Storm log / occurrence has been created and the vehicle / equipment circulated on PNC.

8. Officer Response to 'Call for Service'

8.1 Investigating officers are responsible for:

- Considering if the person reporting should be referred to their bank / financial institution or Action Fraud;
- If the person is vulnerable or the report meets the Call for service criteria:

- Conduct a thorough investigation that will include taking statements and securing all available evidence including CCTV; and
 - 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 district CID.
- Reviewing and applying the Call for service criteria for fraud investigations and ensuring victim's expectations are managed and met accordingly;
 - Providing a rationale on Storm as to whether or not an investigation is recorded, in line with NCRS;
 - Record fraud report on Athena which in turn will provide relevant detail to Action Fraud which records fraud crime nationally, in accordance with the Home Office Counting Rules and National Crime Recording Standards.

9. Crime Evaluation (IMU)

9.1 Crime evaluators are responsible for:

- Reviewing crimes recorded in line with the Call for Service criteria for fraud investigations and ensuring that cases that do not meet the criteria for investigation are evaluated and finalised accordingly;
- For cases reviewed by IMU, recording rationale for not pursuing an investigation after applying the Call for Service criteria, National Decision Model and force policy, particularly in relation to crimes recorded by district staff or as a result of a call for service;
- IMU will register interest for Action Fraud notification.

10. Fraud Investigation Model (FIM)

10.1 All fraud investigations that have been evaluated and accepted as a 'call for service' or referred via Action Fraud for investigation will be allocated to the most appropriate unit or officer to investigate. This is likely to be CID or district staff.

10.2 It is important that a receiving supervisor carries out an initial assessment and evaluation. Factors that should be considered when undertaking the evaluation should follow the development of an initial case theory (hypothesis). The development of this should be based upon the information presented to identify what may have happened. This initial assessment and subsequent stages of the investigation should be consistent with the Fraud Investigation Model (FIM).

- 10.3 The Fraud Investigation Model (FIM) has been developed to take account of the unique nature of fraud. It is intended that this model should bring about a structured and logical approach to the investigation of fraud.
- 10.4 The principles of the model should be central to all Norfolk Constabulary fraud related investigations.
- 10.5 The model, in comparison to other investigative models, identifies that criminality, risk of harm and loss continues following reporting and during investigation and data gathering stage.
- 10.6 The model considers the need to limit the period of harm and loss by stopping the fraudster at the earliest opportunity, placing an emphasis upon opportunities for early disruption and prevention with initial evidence gathering and data collection.
- 10.7 The model recognises the need for a wider consideration for fraud investigation, identifying enablers, opportunities to prevent continued reoccurrence or evolvment of fraud and the need for a more networked response between agencies.
- 10.8 The FIM is contained within [Appendix D](#).
- 10.9 In cases where a supervisor considers that a fraud investigation should not be progressed in considering resources available, government and local policing priorities, and competing needs of other investigations, consultation should occur at Inspector level for decision and rationale.
- 10.10 For investigations appropriate for allocation, the supervisor will allocate to a suitable officer, or raise query of ownership.
- 10.11 Supervisors should consider providing an initial investigative plan to officers allocated. This investigative plan should, in some cases, consider a staged approach, noting that further information is often needed prior to fuller assessment to establish more detailed terms of reference.
- 10.12 Investigative plans should be in keeping with the FIM.
- 10.13 Officers can seek advice from CID or appropriate financial investigators.
- 10.14 Investigating officers will have a continued duty to ensure safeguarding measures are reviewed and remain effective throughout.

11. Escalation process to ERSOU or reallocation within NC

- 11.1 Norfolk Constabulary has adopted the 'principles for escalation' as a means of identifying suitable cases. Operations suitable for escalation are MoRiLE (Management of Risk in Law Enforcement) scored and a MoRiLE rationale document completed (ROCTA11). Rationale for escalation should be specific as well as the support required. (In line with the National Transfers NFIB Instruction) [Appendix G](#).

- 11.2 ROCU (Regional Organised Crime Unit) Regional Organised Crime Threat Assessment (ROCTA) moderates MoRiLE and determines the most appropriate response using the 'principles for escalation' or provides rationale for non-escalation.
- 11.3 Cases requiring National Economic Crime Centre (NECC) or National Lead Force ((NLF) City of London Police) support are submitted direct to NLF by ROCTA.
- 11.4 Cases suitable for ROCU support are presented to ROCU tasking.
- 11.5 Cases not adopted by NLF or NECC are returned to referring Force / ROCU with rationale.
- 11.6 The factors intended to inform assessment decisions relate to serious and organised crime, complexity, need for specialist skill sets, significant loss to large number of individuals, organisations or similar.
- 11.7 Norfolk Constabulary district-based investigations which are considered more appropriate for other NC units will involve supervisor or manager communication with an assessment between those individuals. The considerations should involve factors relating to level or threat, risk and harm posed. As well as complexity and collective capacity.

12. Established Preventative Measures

- 12.1 This section is not intended to duplicate areas of prevention identified through the FIM, but to outline existing and established mechanisms already in existence for Norfolk Constabulary.

Operation Bodyguard

- 12.2 Operation Bodyguard involves the Strategic Business and Operational Services (SBOS) department reporting to a designated Police Inspector monthly figures which help their team identify vulnerable victims.
- 12.3 A prioritisation matrix is used to identify those most vulnerable.
- 12.4 Advice via email or arranged visits to the most vulnerable will then be arranged.
- 12.5 Four Op Bodyguard advocates are deployed in conducting intervention visits across the county.
- 12.6 Details of these visits are recorded on Athena to help track repeat victims.
- 12.7 A results analysis is completed every six months to review repeat victim rates.
- 12.8 Scam Prevention Service / Operation Bodyguard will provide advice and guidance for most vulnerable victims.

Banking Protocol

12.9 This was launched in Norfolk and Suffolk in 2017.

12.10 The protocol identifies that victims, particularly the elderly and vulnerable, are targeted for a range of fraud related offences including courier fraud, romance scams, investment scams and rogue traders, amongst others. The victim is often encouraged to attend the bank in person or withdraw or transfer cash and is regularly accompanied by the offender to do so.

12.11 The primary objectives relate to:

- Identifying individuals tricked into going into banks and withdrawing or transferring funds;
- Creating a standardised method for the prevention of such fraud;
- Provision of victim support to reduce future susceptibility to fraud;
- Apprehension of offenders.

Norfolk minimum standards:

- CAD for deployment;
- ATHENA report;
- Action Fraud report;
- CCTV;
- Victim and witness statements;
- Forensic considerations;
- Crime prevention advice;
- Referrals via MASH if vulnerable adult.

12.12 Partnership members of the Local Organised Crime Group Partnership Board (LOCGPB), collaboratively address organised fraud and other crime types. They work within the four P strands with effective links to ERSOU, Trading Standards, DWP and similar.

12.13 Norfolk Constabulary has been involved in national community anti-fraud campaigns (Take Five), Prevent months for the Over 60s relating to fraud and cyber offences and social media platforms to warn of scams and opportunities to protect against personal fraud. Every district has embedded an Engagement Officer who are able to circulate key messages, including those for fraud prevention and target activity against those most at risk.

13. Resources

- 13.1 Norfolk Constabulary investigations are generated by an officer, or created on Athena by the Investigation Management Unit (IMU) following NFIB referral. They are then allocated out to the most suitable resource – usually CPC or CID. See [Appendix C](#).
- 13.2 With the regionalisation of the Economic Crime Unit (ECU), the large-scale frauds are now investigated by CID, with lower level incidents investigated by uniform resources. The scale of the fraud is not necessarily indicative of whether there is associated vulnerability, so this must be an individual consideration. Norfolk Constabulary already has processes in place that evaluates 'THRIVE'.
- 13.3 Norfolk Constabulary has continued to invest in Detectives attending the Fraud Investigators course and these trained officers are embedded within CID.
- 13.4 Monthly data from National Fraud and Cyber Crime Reporting Centre is routinely compared across our local crime/intelligence recording system (CIS and Athena) to identify repeat victims and ensure correct referrals to support/advice services, as well as local policing intervention where appropriate.
- 13.5 The same level of professionalism is attributed to this as any other investigation, however, other competing and higher priorities may affect timeliness on occasions.
- 13.6 If the investigations are more complex, requiring a greater set of fraud investigation skills, then such enquiries are referred to the joint Norfolk and Suffolk Constabularies' Cyber, Intelligence and Serious Crime Directorate through either the Detective Sergeant or Inspector.
- 13.7 Acceptance of fraud investigations into Cyber and Fraud Department is assessed taking into consideration a number of factors which are defined.
- 13.8 Should an investigation require the services of a Financial Investigator (FI) then the OIC completes an application to the Eastern Region Special Operations Unit (ERSOU) by means of a referral form and an FI will be allocated to assist on a case by case basis. ERSOU will then assess the investigation against their own acceptance criteria.
- 13.9 Access to Regional assets is via Joint Force Tactical Tasking and Coordination Group (JFTTCG).

ERSOU

- 13.10 The Eastern Region Special Operations Unit comprises of two departments whose primary function is the investigation of fraud;

- Regional Economic Crime Unit (RECU);
- Regional Asset Recovery Team (RART).

RECU

13.11 Relevant investigative support requiring specialist financial investigation techniques to Serious and/or Organised Crime investigations by primary service users. Cases are managed by force Serious and Organised Crime Units or equivalent and will be supported from inception. Other cases will be adopted at an appropriate point as negotiated by the OIC, their supervisor and a team leader within the RECU.

13.12 Initial triaging of Suspicious Activity Reports (SARs) and dissemination of relevant information to forces.

RART

13.13 The RART is a six Force resource covering Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Norfolk and Suffolk and divides priority between two areas of Fraud investigation. The RART is then also split into two areas of business, the ACE (Asset Confiscation Enforcement) and MLIT (Money Laundering Investigation Team) teams.

13.14 The ACE team forms part of the Regional Asset Recovery Team (RART) and is Home Office funded. The objective of the ACE team is to take control of the compliance/enforcement process, in cases where orders are expected to be beyond the capacity of the investigating FI to realise, from its earliest stages with a view to:

- Tracking compliance with restraint orders and investigating any breaches to bring about prosecution in conjunction with the CPS.
- Work to assist defendants where appropriate to comply with confiscation orders before the time to pay expires.
- Work to obtain compliance following expiry of the time to pay and where necessary conduct investigations to bring about enforcement action.
- Conduct investigations to support the revisit of orders under Section 22 POCA 2002.

13.15 The MLIT undertake serious and/or complex money laundering and fraud investigations which are referred at force level. The referrals will relate to investigations which, at that time, are not within the force's capacity or capability. The MLIT terms of reference;

The MLIT will respond and deliver Force needs in respect of serious and complex money laundering and fraud investigations that:

- Are tasked by the Regional Tactical Tasking and Co-ordination Group (RTTCG), and

- Are beyond the local investigative capability of that constituent Force, and/or
- The application of specialist money laundering tactics are required in order to effectively deal with relevant criminal entities or nominal(s).

14. IMU Reporting Returns to NFIB

14.1 Once an investigation is finalised within Athena, IMU will send a monthly return to NFIB giving details of the outcome