HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:21/10/2026

2026/998 - Policy

In response to your recent request for information regarding;

For the record would NWP confirm that it is policy to not investigate the following criminal activities;
1, abuse of office.
2, money laundering.
3, loan sharking of a vulnerable client.
4, obtaining moneys with threats of violence

Please see attached Fraud policy.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 19/10/2026

HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

POLICY

ECU FRAUD POLICY

Governance:	**Senior Leadership Team**		
Document Type:	**Policy**		
Policy Owner:	**Head of Crime Services**		
Department:	**Crime Services – Economic Crime Unit**		
Policy Writer:	**DI Economic Crime Unit**		
Policy Number:	**151**	**Version:**	**3.1**
Effective Date:	**15/04/2026**		
Recommended Review Date:	**01/10/2027**		

Governance:	Senior Leadership Team
Document Type:	Policy
Policy Owner:	Head of Crime Services
Department:	Crime Services – Economic Crime Unit
Policy Writer:	DI Economic Crime Unit
Policy Number:	151
Version:	3.1
Effective Date:	15/04/2026
Recommended Review Date:	01/10/2027

CHANGE HISTORY

Version No	Date	Author	Changes	Ratification
1.0		DCI	New policy	SLT
2.0	14/02/22	DC	Scheduled refresh	
2.1	24/04/25	DI	Incorporate pronto changes	N/A
3.1	20/02/26	DI	Refresh	

Contents

1. WHY IS THIS POLICY REQUIRED ..... PAGE 2
2. WHO SHOULD USE THIS POLICY ..... PAGE 3
3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY..... PAGE 4
4. ROLES AND RESPONSIBILITIES ..... PAGE 5
5. THE FRAUD REPORTING PROCESS ..... PAGE 8
6. VULNERABILITY ASSESSMENT FOR VICTIMS OF FRAUD/CYBER ..... PAGE 12
7. FRAUD TRIAGE PRINCIPLES ..... PAGE 17
8. PRIORITISATION OF INVESTIGATION ..... PAGE 18
9. NO INVESTIGATION ..... PAGE 21
10. ALTERNATIVE RESOLUTION FOR FRAUD ..... PAGE 23
11. FRAUD INVESTIGATION PROCESS ..... PAGE 31
12. MONEY MULE PROCESS ..... PAGE 34
13. DECLARATION AND LEGALITIES ..... PAGE 35

1. WHY IS THIS POLICY REQUIRED?

This policy

- Seeks to protect the communities of North Wales who are at risk as a result of fraud.
- Provides a clear and consistent approach in assessing the vulnerability of all victims of fraud across North Wales and thereafter ensure effective support for vulnerable victims.
- Sets out the agreed model for allocating and investigating volume and major fraud offences.
- Provides a triage framework for staff to use their knowledge and discretion to make the most efficient and effective decisions to achieve the best possible result for all victims of economic crime.
- Sets out a model to assist North Wales Police, together with our partners to do the right thing in line with the force strategy. This promotes 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.
- Adopts a consistent and proactive approach in triaging fraud investigations across North Wales thereby reinforcing the National Fraud 4 P Strategy in tackling fraud and cybercrime.
- Provides clear and consistent standards to ensure the effective supervision, management and prioritisation of fraud investigations.
- Is aligned to our force priorities which are
    - **Being visible and engaging with our communities**
    - **Focusing on the basics of fighting, preventing and reducing crime**
    - **Providing an excellent service to victims**



2. WHO SHOULD USE THIS POLICY?

This policy should be used by all North Wales Police Officers, police staff and members of the office of the Police and Crime Commissioner. Individual managers and supervisors are responsible for ensuring that this policy is applied in their area of operations.

This policy includes:

- An outline of the role of the fraud triage officers in the reviewing and allocation of fraud investigations
- An outline of the role of the Financial Abuse Safeguarding Officer (FASO) in assessing and protecting vulnerable victims of fraud
- A brief overview of the role of the Cybercrime unit within the Protect model
- Many of our documents have now migrated to Pronto and therefore all previously used paper copies have been removed from this document to prevent their use in error.
- An outline of the agreed National Fraud Reporting process whereby North Wales Police will direct any person wishing to report a fraud to the Report Fraud contact centre unless the case meets the agreed call for service criteria as outlined in the CRE.
- A requirement to follow the College of Policing Fraud Investigation Model (FIM) (See Appendix 1) for relevant fraud investigations
- Direction, together with relevant information, outlining the Force's stance on dealing with victims of fraud and fraud investigations
- A corporate framework for triaging fraud cases (see appendix 6 and appendix 7)
- Process maps for high harm / high risk fraud MO's

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

Fraud is a type of criminal activity defined as:

> *'Abuse of position, or false representation, or prejudicing someone's rights for personal gain'.*

Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party.

The majority of criminal activity classified as frauds are captured by offences under the Fraud Act 2006.

Some useful documents to read in conjunction with this policy are:

- National Fraud Strategy
- North Wales Police Economic Crime Strategy 2025-28
- College of Policing APP on investigating fraud
- Blackstone's Investigation of fraud and economic crime
- HOCR and NCRS, Crime Recording Guidance Framework
- R2 Fraud Escalation Grid
- NWP Crime Management Plan

4. ROLES AND RESPONSIBILITIES

4.1 Force Control Room (FCC)	• To follow the fraud CRE (see appendix 4). • To follow the fraud process map (see appendix 3).
4.2 Police officers / PCSO	• To follow the fraud process map (see appendix 3). • Complete relevant ICR and DAN documents as required • Progress fraud investigations as directed at triage as required • Support safeguarding as required.
4.3 IMT	• Follow the fraud process map. (see appendix 3) • Refer all frauds reported to ECU for review. • Gather all relevant information and document on ICR
4.4 FASO (Financial Abuse Safeguarding Officer)	• Assess and protect vulnerable victims of fraud. • Sharing of data with regards to banking protocol with UKFIU. • To identify and highlight occurrences that have an element of vulnerability and assess the risk to the victim. • To complete safeguarding referrals to relevant third parties. • To complete and submit Vulnerable Victim Notices to the financial sector. • To provide bespoke protect advice to attending officers for vulnerable victims of fraud to enable protect advice to be delivered. • Submit disruption requests on bank accounts, telephone numbers, email addresses, social media accounts and websites suspected to be used in fraud. • If required to conduct visits to vulnerable victims of fraud.
4.5 Fraud PCSO Engagement Officer	• Support the targeted delivery of protect advice to the most vulnerable victims • Gather information from victims and witnesses of fraud that will assist in the disruption of economic crime • Deliver in person advice to victims of fraud
4.6 Cyber protect / pursue officer(s)	• Attend ECU briefings and share daily updates on existing demand. • Support cyber enabled investigations with bespoke advice in line with the 4P Plan • Lead on Cryptocurrency related economic crime • Support Protect advice messaging

4.7 Economic Crime Unit (ECU) Fraud Triage	• To receive all fraud investigations from Report Fraud. • To review and triage all fraud occurrences on RMS that have been tasked to the ECU Fraud Triage Pot reported via FCC, officers or via third parties. • Following triage to establish if the reported occurrences are to be investigated, allocated to FASO for safeguarding, NFA or transfer to Report Fraud using the CAT fraud triage matrix (see appendix 2). • To conduct desktop-based investigations of offences of fraud in line with the FIM (see appendix 1). • To allocate fraud investigations to the relevant department following triage. • Provide advice and assistance to Investigating Officers/ Supervisors. • To assess and direct investigations that relate to fraud, money laundering, bribery and corruption and election malpractice in line with capacity. • Report the details of the crime to Report Fraud in accordance with NCRS (National Crime Recording Statistics). • Record the Report Fraud crime number in the relevant occurrence ID tab on NICHE. • To review all fraud cancellations, to add a rationale to the OEL and to request a cancellation via the NCRAS portal. • To request transfers via the trans crime process on the NCRAS portal. • To provide investigative advice with regards to election malpractice.
4.8 NWP Crime data integrity unit (CDIU)	• To receive all fraud, pursue investigations from N-CAS and create occurrences on Niche • To follow HOCR for when a fraud should be recorded and task ECU fraud triage NICHE pot. • CDIU also classify all fraud call for service from ICAD with NFIB crime codes.
4.9 FCIR (Force Crime and incident registrar)	• Review and ratify all outcomes ensuring that all incidents and crimes are recorded accurately and within directed timescales.

4.10 ECU DI	• Retains overall responsibility for updating the Fraud policy. • Complete dip sampling of all active fraud investigations as per process map (see appendix) • Engage with regional and national partners to ensure NWP are aware of national trends and are meeting national expectations for the delivery of fraud investigations. • Ensures the force have access to subject matter experts with the relevant experience to provide direction and advice as required. • To be the final arbiter of disputes in terms of allocation and provide a robust rationale in line with the Code of Ethics and Force Priorities. • Ensure that staff within the ECU and all other staff with fraud responsibility receive appropriate training.
4.11 Managers / Supervisors	• Ensure this policy is applied in your area of operations. • Ensure all fraud occurrences are tasked to ECU Fraud Triage once first service has been carried out to ensure compliance with NCRS. • Ensure VCOP compliance is adhered to. • Where appropriate seek further ECU guidance when required. • If a case has been under investigation for over 12 months it is recommended that supervisors notify ECU DI and request a review. This may assist in refreshing parameters and also assist the force to better understand factors affecting case progression thus promoting organisational learning.
4.12 Senior Managers	• Ensure that the force's response to fraud is scrutinised appropriately. • Ensure Fraud is included in all relevant governance forums • Promote and support a wider understanding of Economic Crime and its impact on our communities

5. THE FRAUD REPORTING PROCESS

5.1 Reporting Fraud Offence – Report Fraud

Report Fraud (the UK Police's national reporting centre for fraud and cybercrime) send reports of fraud offences onto the National Fraud Intelligence Bureau (NFIB) operated by the City of London Police. The NFIB collates and analyses intelligence on fraud and decides thereafter which cases are referred to police forces for investigation.

If the victim is reporting a fraud, the CRE process should be followed by the Force Control Room (appendix 5). Should the CRE not be met then the FCC should be advising the victim to report the matter to Report Fraud and creating the call as a contact record.

5.2 CRE

5.2.1 Force Control Room / Any Officer receiving a report of a fraud	• Report Fraud stipulate that the following circumstances would warrant a police response known as a Call for Service. 1. An offender has been arrested for a fraud offence. 2. The local offender is committing, or has recently committed, a fraud offence at the time of the call for service. 3. The suspect is known and a local suspect. 4. The victim is vulnerable. • Create on ICAD a report of fraud to launch the CRE process. • On completion of the CRE, should the CRE not be met, a victim should be advised to report the matter to Report Fraud. • Following completion of the CRE, follow the Fraud Process Map (appendix 6). • For offences not recorded by Report Fraud, see sections 5.3 & 5.4 below.
5.2.2 Initial Investigating Officer & Supervisors	• North Wales Police will follow the National Fraud Investigation Model (FIM) (see Appendix 2) • Consider if the person reporting should be referred to their bank/financial institution and/or Report Fraud. • If the case meets the CRE criteria then you should: • Conduct a thorough initial investigation. This will include taking statements and securing all available evidence. • 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 from ECU Fraud Triage or via the ECU SharePoint page.
	• Once first service is complete, the occurrence should be tasked to the NWP ECONOMIC CRIME UNIT FRAUD TRIAGE pot for triage. • In order to comply with the NCRS, a Report Fraud reference number must be obtained at the earliest opportunity which can be obtained from ECU Triage Officers. • If the victim has self-reported to Report Fraud, the OIC is responsible for obtaining the reference number at the time of first service.

5.3 Offences not recorded by Report Fraud

Do NOT report the following fraud offences to Report Fraud

- making, supplying or use of articles to commit fraud
- possessing/controlling article(s) for use in fraud
- possession of false documents
- theft of fuel*
- Identity theft
- forgery or use of drug prescription
- fraud or forgery relating to vehicle or driver records
- other forgery
- blackmail / sextortion (however there may be a cyber element)

*unless there is a clear element of deception by the offender at the time of the offence

5.4 PNC Lost/Stolen Report – Theft of Vehicles / Plant

If the fraud offence involves theft of motor vehicles or plant equipment,

- Create an ICAD log/occurrence
- Circulate the vehicle/equipment on PNC.

(Report Fraud does not have access to the Police National Computer (PNC) and therefore will be unable to record crimes where a PNC 'registered item' requires an entry on PNC (i.e. vehicle, plant, machinery etc). Police will be responsible for reporting these offences to Report Fraud, and making the relevant PNC entry, i.e. LOS, PNC, Interest etc).

5.5 Role of the CDIU in Recording Fraud Occurrences

The crimes disseminated for prevent or pursue are sent to NWP via the NCRAS portal. CDIU supervisors and the ECU Report Fraud SPOC have access to this portal.

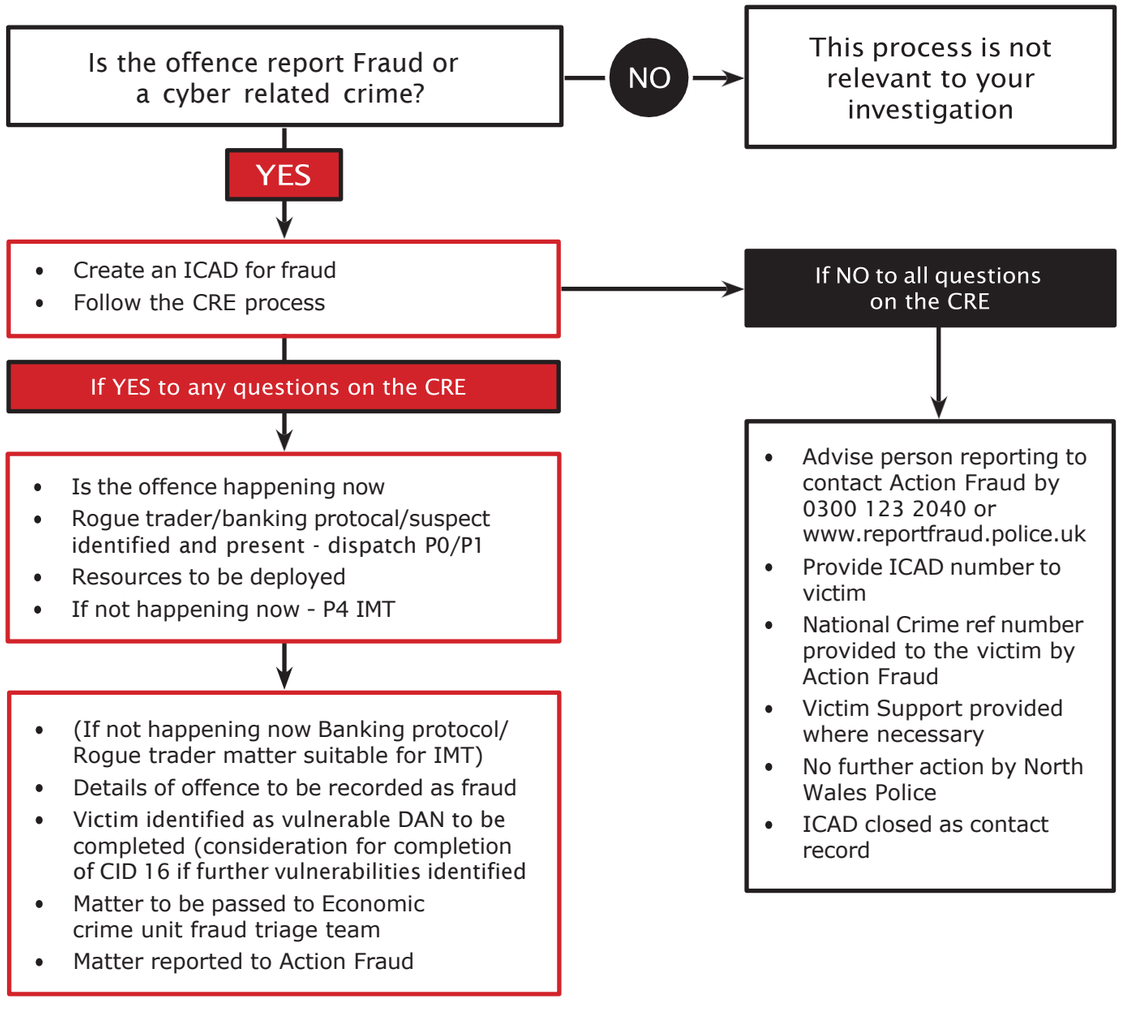
CDIU will record all pursue disseminations onto RMS, which will then be allocated following triage for investigation.

CDIU will also record all 'call for service' frauds on RMS or where the CRE has been met and apply a classification in line with HOCR NFIB codes.

ECU Report Fraud SPOC will record all protect disseminations which will be reviewed by FASO's prior to allocation for safeguarding.

All Transfer of Crime / Cancellation requests in relation to Report Fraud must be submitted by the ECU Report Fraud SPOC via the NCRAS portal.

5.6 North Wales Police Initial Fraud Reporting Process Flowchart ***



5.7 Live Cyber Attack

If a business, charity or organisation is under a live cyber-attack the victim should be advised to call Report Fraud on 0300 123 2040 immediately.

All other reports of fraud should be made to Report Fraud via their website www.reportfraud.police.uk or by telephoning 0300 123 2040.

6. VULNERABILITY ASSESSMENT FOR VICTIMS OF FRAUD/CYBER

In accordance with HOCR location of crime rules, the suspect's location normally dictates which force investigates the crime (See Section 11). As such many frauds reported by victims who reside in North Wales are never disseminated to North Wales Police for investigation. However, the Fraud Investigation Model recognises that fraud can be disrupted by addressing the needs of the victim. A proper assessment of those needs can assist in making it more difficult for the offender to target that victim and thereby reduce the likelihood of them suffering further loss. This approach is in line with the force's priorities to provide an excellent service to victims and focusing on preventing and reducing crime.

The force has invested in our safeguarding capability and have officers assigned to the Protect role for both Fraud and Cyber. To safeguard victims of fraud in North Wales, the FASO assesses all North Wales victims of fraud crimes for repeat victimisation and/or vulnerability. This assessment will also be assisted by ECU cybercrime protect/ prevent officer(s) who will review all the relevant NFIB stats class for any evidence of vulnerability or if they are aged 70 and above as classified in the vulnerability review. If these are identified as vulnerable the ECU cyber officer will follow the ECU FASO vulnerability process as per Section 6.4.3. This is in accordance with Force Policy and Operation signature and in addition to the referrals that are sanitised by ROCU as per Section 11.5.2

NFIB50	Computer Misuse Crime
NFIB50A	Computer Viruses\Malware\Spyware
NFIB51A	Denial of Service Attack
NFIB51B	Denial of Service Attack Extortion
NFIB52A	Hacking-Server
NFIB52B	Hacking-Personal
NFIB52C	Hacking-social media and E-mail
NFIB52D	Computer Hacking – PBX/Dial Through
NFIB52E	Hacking (Extortion)

6.1 Operation signature overview

Operation Signature is a standardized method introduced to identify and support vulnerable victims of fraud. It provides preventative and supportive measures intended to protect victims and safeguard them from further targeting. An important strand of Operation Signature is its wider messaging and prevention advice, working with statutory and voluntary agencies to influence change.

The aim of Operation Signature is to work together to ensure that:

- Police deliver an excellent quality of service to vulnerable victims of fraud.
- Vulnerability is identified at the earliest opportunity and those requiring additional support are provided appropriate signposting/referrals.
- Available investigative opportunities are pursued in line with the Fraud Investigation Model and Force/National policies and procedures.
- Preventative measures are identified and implemented, with an emphasis on maximizing protection for the victim and reducing the risk of repeat victimization.

6.2 The Vulnerability Review

ROLE	ACTION REQUIRED
6.2.1 FASO	• Review Report Fraud and FCC data • Assess each case for any identifiable vulnerability under the following categories: Age 70+ Mental health concerns Disability (as per the Equality Act definition) Significant financial vulnerability Repeat victim Victim of recognised high harm fraud Significantly isolated or technically unaware • Review available intelligence including Report Fraud data to identify repeat victims (including repeat businesses).

6.3 Identified Vulnerable Victims

ROLE	ACTION REQUIRED
6.3.1 Force Control Room / Any Officer received a report of fraud	• The Force Control Room Staff will follow the CRE for Fraud reports (see appendix 5) • Any other officer receiving a report of fraud regarding a victim 70 years will create an occurrence on NICHE as a fraud. If they are identified as vulnerable or significantly affected and it has not been previously referred to North Wales Police, they will receive a visit from a PCSO or Police Officer for a Direct Assessment of Needs questionnaire (DAN) to be completed. The victim will also receive Crime Prevention advice on that visit to prevent repeat victimisation.
6.3.2 PCSO/ Police Officer	• Complete a face-to-face visit with the victim and carry out first service. • Complete Direct Assessment of Needs (DAN) on the Pronto system. • Complete the ICR document on the Pronto system. • Collate all relevant information available for disruption and national safeguarding purposes which should include: Time, date and location of any offence Suspect phone numbers Suspect emails addresses Suspect webpages Suspect social media profiles Suspect bank account details / crypto wallets Details of other apps used • When Romance Fraud is reported, ensure the Romance Fraud Questionnaire is completed. • Where suspects have physically attended, consider House to House and CCTV enquiries. • Complete CID16 referral to notify other agencies • Provide Crime Prevention advice and documentation as appropriate to the circumstances.
6.3.3 FASO	• Review the Direct Assessment of Needs and identify and assess any ongoing risk to the victim or their finances. • Raise any significant concerns to a supervisor where significant risk is identified. • Outline any additional safeguarding or support required from NPT or LPS and task back to the OIC or relevant allocations NICHE pot for action.
	• Where necessary, contact the victim directly, either remotely or face to face, to address any high-risk concerns identified or offer speciality advice and support. • Utilise financial intelligence to identify risk and support victims. • Complete referrals to Victim Help Centre • Identify and prioritise disruption opportunities for phone numbers, websites, emails and bank accounts. • Ensure all disruption activity relating to suspected organised crime is identified for APMIS recording. • Ensure relevant referrals are made to the NFIB in relation to high harm fraud. • Seek specialist support from internal departments where relevant. • Attend multi agency meetings and strategy meetings with external agencies. • Ensure the matter has been reported to Report Fraud. • Submit Vulnerable Victim Notices to banks where it is identified they need to safeguard the victim further. • Provide information on the current reimbursement schemes available and support victims with reimbursement requests where there is no other support in place. • Consider VARM process for the most serious repeat cases.

6.4 Victims identified as non-vulnerable

Operation Signature is a standardized method introduced to identify and support Victims may initially be identified as non-vulnerable but following assessment of the facts, it may later be deemed that the victim is vulnerable and requires additional support. This could be where there is:

- Significant financial loss
- Other identified factors such as domestic violence or controlling and coercive behaviour
- Suggestion of money muling
- Links to MDS

A victim can be identified as vulnerable at any stage e.g. at the time of reporting, during the first service, at the time of triage or during follow up contact.

ROLE	ACTION REQUIRED
6.4.1 FASO	• Monitor all ICAD Fraud reports to ensure vulnerability has been correctly identified by FCC. • Monitor all Banking Protocol incidents to ensure vulnerability is correctly identified (see 6.5) • Re-review any case raised to the ECU directly by officers via the ECU inbox. • Assess cases identified at the point of triage where vulnerability is identified. • Ensure all disruption activity relating to suspected organised crime is identified for APMIS recording.

6.5 Banking Protocol Overview

The Banking Protocol is a national scheme between the Police and financial sector organisations (banks, building societies and the Post Office). The aim is to identify customers who are in the process of being defrauded and implementing safeguarding procedures to prevent victimisation and loss of funds.

The Banking Protocol is an effective initiative and the minimum police response to such an incident, which is an urgent call for service, must be a recorded crime and a criminal investigation and referral into the Operation Signature process completed.

6.6 Victim(s) Identified as High Risk

ROLE	ACTION REQUIRED
6.6.1 FASO	• Contact the relevant duty sergeant/district inspector for the area concerned so that effective safeguarding and support can be implemented for the victim concerned.

This system is in keeping with the Safer North Wales principle in the victims' best interest. It provides a framework for staff to use their knowledge and discretion to make the most efficient and effective decisions to achieve the best possible result for any victim of economic crime.

It intends to address the growing threat that fraud and cyber enabled fraud poses to our communities within North Wales. The triage framework enables a problem-solving approach to target individuals and groups that cause threat.

7. FRAUD TRIAGE PRINCIPLES

7.1 The Fraud Triage Matrix

North Wales are committed to ensuring that fraud investigations are reviewed by subject matter experts and allocated to the appropriate resource. This approach not only complies with the NECC R2 national approach but also allows for all fraud investigations within the force to receive SME direction at the earliest opportunity.

The fraud triage matrix is based upon the crime allocation triage (CAT) system that was introduced for the scoring and allocation of criminal investigations. The relevant crime is reviewed by a DS and those scoring above 55 are allocated to a PIP2 investigator. The force is familiar with this approach therefore the Fraud triage has been designed with a similar methodology for greater understanding.

The matrix considers vulnerability, types of fraud, threat, harm, risk to the victim/ business and any opportunities that are available to disrupt the suspect(s). Decision making in terms of investigation is therefore underpinned by the principle of threat, harm and risk and therefore the risk of further offences should be at the forefront of decision making at all stages of the triage review.

Scoring will be determined upon the answers that the reviewer selects. The reviewer will decide if the matter is for safeguarding, investigation, transfer to NFIB, transfer to another force or NFA.

Any occurrence scoring 55 or over are for a PIP level 2 investigation and will be allocated to the respective CID area. Should an investigation require additional resources above and beyond the capacity of a Divisional CID team then ECU will then refer the matter to L2 tasking. Within L2 tasking the matter will then be considered for adoption with appropriate resourcing in force or if there is a capability gap will be referred to the Region for consideration of adoption.

The relationship between Regional and Force Economic Units is constructive and early engagement is encouraged to assist in identifying and resolving any capability gaps prior to formal adoption procedures.

8. PRIORITISATION OF INVESTIGATION

8.1 Prioritisation of Investigations

To investigate – initial considerations

- The victim(s) are believed to be vulnerable (e.g., older people, people with disabilities and socially isolated individuals including other protected groups under the Equality Act 2010) and potentially at risk of repeat offences or a continued course of criminal conduct.
- Frauds that have a significant impact on the victim(s) (e.g., 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 linked series
- The offenders are part of an organised crime group and the activity reported would score 'high' on THR 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, 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.

8.2 Prioritisation of Investigations

North Wales Police will never seek to blame any victim of crime for the actions of others. Fighting, preventing and reducing crime is a force priority and any rationale not to investigate must justify how our response as an organisation can deliver this should no further investigation take place. However, there will be circumstances where it is appropriate not to investigate further, and the following are initial considerations that will assist the reviewing officer to provide a rationale at triage stage.

- The investigation would require a significantly disproportionate level of resources to bring the case to a conclusion and would adversely impact upon our ability to investigate other crimes.
- The complainants are not willing to support a prosecution due to low level impact on them or where they have been obliged to report the crime by a financial or other institution so that they can be compensated appropriately. For example, when the fraud does not potentially involve other unidentified victims or where a bank/financial institution/company have repaid the victim and the bank/financial institution/company is not pursuing a complaint. (e.g. contactless transactions)
- 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 resourcing of the investigation.
- The complainant has pursued civil recourse and has subsequently turned to the police for a criminal investigation because of dissatisfaction with the civil remedy
- Significant delays to the investigation will be caused by the location of key evidence elsewhere.
- Where clear and obvious safeguards are in place to prevent fraud that the complainant was aware of but proceeded to engage.
- (PSR Authorise Push Payment guidelines are an example where this may be relevant, but caution should be exercised given that fraud by its nature often includes activity designed to exploit individuals).
- Incidents where the complainant has played an active role in the fraud. (clearly where there is suspicion of coercion or duress this will not apply).
- Cases where the complainant's motive for making a complaint are clearly malicious or designed to deflect attention from the complainant's own involvement in criminality. (such a case may nevertheless merit investigation especially where other victims may be identified).
- Cases where complainants are not prepared to co-operate fully with the investigation unless there are grounds to suspect that they are being targeted in multiple ways e.g. Controlling behaviour, Modern Day Slavery or Romance Fraud
- 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 unless there are exceptional circumstances. As a rule, this applies to any fraud that occurred over 2 years previously, however, this will always be considered objectively.

Fraud Triage will give due consideration to the score provided and what is required for the victim. A decision is then made to allocate to either:

- PIP1 Investigator
- PIP2 Investigator
- Cyber Crime Team Officer
- Economic crime unit investigation
- To set up a dedicated investigation team
- Request adoption of the case by regional resources in line with Morile scoring to address a capability issue.
- or to consider no investigation or alternative resolutions

9. NO INVESTIGATION

If the decision is to not investigate: -

- The triage officer will review the material and pass the file to the Fraud Sergeant with a recommendation.
- The Fraud Sergeant will review the case and confirm that they authorise allocation or NFA as appropriate.
- The Fraud Sergeant will ensure that the matter has been appropriately recorded, and a Report Fraud reference is linked to the occurrence.
- If the matter is to be NFA the Fraud Sgt will ensure that the complainant has been updated and provided with an appropriate rationale.
- When closing the occurrence, the Sergeant will ensure that the appropriate outcome is applied in line with HOCR rules.
- Where appropriate the named suspect(s) will receive an appropriate letter of warning regarding their behaviour. This is known as a 'cease and desist' letter (see Appendix 4) which must be authorised by a Detective Sergeant or above with the rationale for issue endorsed on the occurrence.
- When a 'cease and desist' process is used Outcome type 22 is to be used to file the case on RMS and RFAS advised.

When a decision is made at supervisor or management level that no further investigation against the suspect is in the public interest the below considerations should be noted: -

- Outcome 21 is not appropriate for 'serious' offences such as domestic abuse, hate crime, child abuse or any indictable only matter. If, in exceptional circumstances, use of Outcome 21 is deemed appropriate for a 'serious' offence, this must be ratified by the Force Crime and incident Registrar (FCIR) at the earliest opportunity.
- Only decide to apply Outcome 21 after careful consideration which is documented in a comprehensive entry on the RMS OEL. Outcome 21 can only be applied when authorised by a supervisor at a point of decision. The victim must be informed of the decision in writing/email.
- Outcome 21 will only be utilised in very exceptional circumstances.

ROLE	ACTION REQUIRED
9.1 Force Crime and incident Registrar	• Periodically review the application of Report Fraud reference numbers and outcome codes to ensure compliance with HOCR standards • Raise any issues of non-compliance via the appropriate CRUG forum.

Standards of HOCR compliance are reported at force level meetings.

The views of the victim (or their representative) will always be an important consideration when taking the decision not to investigate an offence where there is a named suspect. Their views must be recorded in clear and auditable manner.

There are exceptional circumstances when, contrary to the victim's wishes, it would not be in the public interest to investigate an offence. When this is the case, the decision must be endorsed by a supervisory officer. Fully document the rationale for this decision in the crime record OEL, confirming the victim has been made aware of this outcome. The ECU DI will dip sample cases screened out at triage stage to ensure that decision making is consistent and justifiable.

Regard must be given to the public interest test considerations set out in the Code for Crown Prosecutors Para 4.12 a-g: The key points are as per Appendix 7.

The guidance around appropriate use of outcomes is provided by the FCIR, readers of this policy should direct themselves to the HOCR / NCRS Recorded Crime Outcome Tool and the Crime Recording Framework.

The Sergeant within the ECU fraud triage team will review all requests for cancellations and transfers of fraud occurrences. They will add an entry onto the OEL and if the matter has already been reported to the RFAS the SPOC will request a cancellation of that crime which is held by the RFAS. Once confirmation of a cancellation is received the SPOC will send a task to a DDM (Designated Decision Maker).

10. ALTERNATIVE RESOLUTION FOR FRAUD

As above reference is made to disruption, joint agency working and civil resolution. Within this section, individual types of fraud crime will be highlighted with specific examples of potential alternative resolutions. Each report of fraud must be treated on its merits and on a case-by-case basis. This category includes:

- Cyber Enabled Volume Fraud
- Mass Marketing and Miscellaneous Fraud
- Investment and Banking Fraud

This is not an exhaustive list. It must be used in conjunction with the fraud triage and priority sections of no further investigation of the policy to justify an alternative to a standard criminal investigation. All reasoning must be fully endorsed on niche occurrence OEL for future scrutiny and transparency.

10.1 Cyber Enabled Fraud

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Advance Fee / Ticket Fraud / Telecommunication scams / Internet Consumer Fraud This is the most common fraud type dealt with by North Wales Police. Fraudsters target victims to make advance or upfront payments for goods or services that do not materialise using the internet or telephony.	• Refer to Trading Standards to use bespoke powers if they wish to proceed • Submit intelligence accordingly on Niche • Advise victim of outcome and offer crime prevention advice • Refer to online platforms own investigation teams for resolution. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Online Dating / Romance Fraud This preys on potentially vulnerable people in our community whereby the victim is led via development of a long-distance e-mail or phone relationship into believing they are in an intimate relationship with someone they have never met face to face, building up enough emotional attachment to ask for money to be sent to them for fictitious reasons.	• Ensure safeguarding around the victim is in place and provide crime prevention advice. Advise that sending further monies to the suspect is potentially a *money laundering offence*. • Submit intelligence accordingly via Niche with correct dissemination • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption
Mandate Fraud This type of fraud is committed when someone gets a member of the public or business to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation they make regular payments to either by sending targeted or random e-mail requests via the internet (phishing) or phone.	• Submitted intelligence accordingly on Niche RMS • Advise victims of outcome and offer crime prevention advice • Clearing banks have their own investigation and resolution departments. Consultation may be required with them regarding their role in respect of indirectly facilitating fraud. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption
Gambling Fraud This type of fraud involves the fixing of odds or results to deceive bookmakers or members of the regulated gambling sector.	• Consider referral to Gambling Commission (the regulatory body in this sector) to ensure that the member is not complicit and provide bespoke crime prevention advice to the member. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Intellectual Property Fraud This is when fake goods are passed off as originals and effects many industries including health, music, film, fashion and fragrances.	• Work with partners to identify and disrupt those engaged in the sale of counterfeit goods • Refer all intelligence to the Intellectual Property Office • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption • Refer to FACT (Federation Against Copyright Theft) if music or film related offences • Promote protect Messaging

10.2 Mass Marketing and Miscellaneous Fraud

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Consumer fraud/ Advance Fee / Ticket Fraud / Telecommunication scams / Internet Auction Fraud This is the most common fraud type dealt with by North Wales Police. Fraudsters target victims to make advance or upfront payments for goods or services that do not materialise using the internet or telephony.	• Refer to Trading Standards to use bespoke powers if they wish to proceed • intelligence submission is considered • Advise victims of outcome and offer crime prevention advice • Online platforms e.g. eBay and Gumtree as well as payment facilitators (e.g., PayPal) have their own investigation and resolution departments. Consultation with them may be required regarding their role in respect of indirectly facilitating fraud. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Mandate Fraud This type of fraud is when someone gets a member of the public or business to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation they make regular payments to either by sending targeted or random e-mail requests via the internet (phishing) or phone.	• Submit intelligence accordingly on Niche RMS • Advise victims of outcome and offer crime prevention advice • Clearing banks have their own investigation and resolution departments. Consultation may be required with them regarding their role in respect of indirectly facilitating fraud. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption
Bogus Tradesman Fraud This preys on potentially vulnerable people in our community whereby the victim is tricked or pressured into buying goods or services that the victim does not want or something that is poor value for money. In the exceptional cases where it is considered appropriate not to investigate a case within this category, the authority of the local Divisional Detective Sergeant should be sought.	• Ensure safeguarding around the victim is in place and give crime prevention advice • Refer to Trading Standards to use bespoke powers if they wish to proceed. • Submit intelligence accordingly on RMS.
Charitable Publication Fraud Charitable Publication Frauds occur when a telesales agent calls a business selling advertising space in a bogus publication for a seemingly good cause.	• Disruption visits to business premises with Trading Standards and DWP and criminality notices served • If the business is limited (Ltd) company then Companies Investigation Branch of Department for Business, Energy & Industrial Strategy should be consulted to wind up the business in the public and disqualify directors of the company • Submit intelligence accordingly on niche • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Insurance Fraud Insurance related fraud happens when false claims are made to insurance companies.	• Refer to City of London Police's Insurance Fraud Enforcement Department (if high volume and organised criminality) • Submit intelligence accordingly on RMS • Advise victim of the outcome
Mail Scams Legitimate mailboxes and post redirections can be used in the application of fraud.	• Referral to Royal Mail Investigations Unit to use bespoke powers if they wish to proceed • Intelligence to be submitted accordingly on RMS • Victims to be advised of the outcome and crime prevention advice offered
Money Laundering & Movement This is when proceeds of crime from fraud, or money needed to fund fraudulent activity is moved either using virtual payment systems or by the use of money mules, or when fraudsters buy stolen credit cards or bank account details.	• Intelligence to be submitted accordingly on niche • ECU Financial DS to review for potential civil case. • Referral to HMRC/DWP • Money mules are often victims and require safeguarding and prevention advice. Invariably their involvement requires investigation to eliminate or implicate before an alternative disposal can be considered. • Cease and desist notice to suspect if appropriate.
Long/Short Firm Fraud This is when criminals set up an apparently legitimate business, develop a relationship with suppliers/wholesalers and once having won their trust place several large orders before disappearing with the goods to sell elsewhere.	• Disruption visits to business premises with other agencies. • Intelligence to be submitted accordingly on RMS • Victims to be advised of the outcome and crime prevention advice offered

10.3 Investment and Banking Fraud

TYPE OF FRAUD	POTENTIAL ALTERNATIVES TO INVESTIGATION MAY INCLUDE THE FOLLOWING:
Account Takeover Fraud This type of fraud occurs when a criminal poses as a genuine customer, gains control of an account and then makes unauthorised transactions.	• Referral to the victim's bank's fraud investigation team to close account and restrict use • Referral to Dedicated Cheque and Plastic Card Unit (DCPCU) to investigate if linked or volume offender(s) • Intelligence to be submitted accordingly on niche • Victims to be advised of the outcome and crime prevention advice offered • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption
Credit Card/Bank Card/ Cheque Fraud This type of fraud occurs when personal information is stolen from a card, or the theft of the card itself leads to unauthorised transactions. (RF number per account not per victim)	• Referral to the victim's provider's fraud investigation team to close account and restrict use • Referral to DCPCU to investigate if linked or volume offender(s) • Intelligence to be submitted accordingly on RMS • Victims to be advised of the outcome and crime prevention advice offered. • The following may be appropriate tactics for disrupting this crime type Telephone number disruption Email disruption Website disruption Bank account disruption Social media disruption
Investment Frauds This type of fraud comes in a variety of guises; however, the basis of the offence is the same with potential investors giving money on the assurance of achieving a return and then losing their investments. Due to the prevalence of these types of offences there are multiple government regulatory bodies and alternative law enforcement agencies where these cases could be referred. A selection of offences and appropriate specialist investigative bodies are listed below. False Accounting Fraud – HMRC/ DWP/CIB/Insolvency Service Bankruptcy Related fraud – Insolvency Service Business Opportunity/Trading Fraud – FCA/CIB/Trading Standards Insolvency Related Fraud – Insolvency Services Ponzi/Pyramid Scheme Fraud – FCA/CIB Property Investment Fraud – FCA/CIB Land Banking Fraud – FCA/CIB Loan Scams – FCA/Trading Standards Mortgage Fraud – FCA/SRA Pension Liberation Fraud – Pensions Regulator.	• If cryptocurrency based, consideration of Chainalysis research to identify movement of funds and facilitate recovery of lost property. • Disruption visit to business premises with appropriate above agencies and criminality notices served • Intelligence to be submitted accordingly on RMS • Victims to be advised of the outcome and crime prevention advice offered • Investment fraud is a potential High Harm fraud so any intelligence or disruption opportunities should be highlighted via ECU tasking.

10.4 Prosecution as Money Laundering

It may be appropriate at triage stage that, due to the category and priority of the offence, it is most efficient and effective to investigate the matter as a money laundering case as opposed to the fraud offence. ECU Financial DS should be notified so a POCA asset review can be undertaken and an investigation strategy formulated.

ROLE	ACTION REQUIRED
10.5 Fraud triage officer	• Provide rationale and direction • Provide guidance and advice to investigators in relation to points to prove alongside the relevant investigation strategy.

11. FRAUD INVESTIGATION PROCESS

RFAS allocate crime for investigation based on these 5 principles:

1. The police force area covering the location of the fraudulent operation/ suspect's address or for Business related fraud the office address of the employee or if no office address, the Head Office of the company.
2. The police force area with the greatest number of individual usages or offences
3. The police force area where the first offence was committed
4. The police force area where the victim resides or works.
5. In the unlikely event that it is impossible to determine a Force Area using these principles the NFIB will determine a Force Area.

All fraud investigations should be subject to a triage process within North Wales. As part of this process, the reviewing officer should ensure this case has been appropriately disseminated to North Wales Police by the RFAS and if not, this will be challenged by the CDIU supervisor or by the by the Fraud DS at the earliest opportunity or through the Force Crime & Incident Registrar or Report Fraud SPOC.

Following assessment of the category and priority, if the report is deemed suitable for investigation, then it will be assigned for investigation with an investigation strategy to the appropriate department.

Suitable cases will be scored and assigned to the relevant investigation teams:

- PIP 1 investigator
- PIP 2 investigator LPS
- PIP 2 investigator PVPU
- Economic crime unit cyber-crime team protect/pursue officer
- Economic crime unit fraud investigators
- to set up a dedicated investigation team
- Request adoption of the case by regional resources in line with Morile scoring to address a capability issue.
- or to consider no investigation or alternative resolutions

11.1 Exceptions

Reports of fraud offences received from our safeguarding partners (e.g. Adult Social Care) with significant safeguarding issues requiring a specialist unit will take primacy (e.g., financial control of domestic abuse victims or financial abuse of a vulnerable adult or child in a care home). These cases will need to be forwarded to the ECU for a fraud triage to take place upon these occurrences.

ECU will then consider the financial offences and provide direction in line with the fraud policy and task the occurrence as appropriate. Where there is a crossover of offences the reviewer will engage with the relevant PVPU department to ensure that all relevant offences have been considered.

Due to the national approach to Cyber Dependent Crime, all Cyber Dependent offences received by Report Fraud are processed by RFAS and allocated to the most appropriate force. Therefore, offences categorised as Cyber Dependent but without a fraud element are received by Cyber Crime Team for allocation. These cases are typically Denial of Service (DOS) Extortion attacks on the computer systems of small businesses. The most common MO is to disable the businesses computer system and demand monies (crypto currencies) in return for release of their computer system. Allocation of these cases is managed by the Cyber Detective Sergeant.

11.2 Escalation

As per the Crime Allocation Procedure, a common-sense approach is taken regarding allocation of viable fraud investigations. Building effective, collaborative relationships between the Economic Crime Unit, Patrol Officers and Detective teams is key to ensuring open discussions in the interest of the complainant and our community to determine the most appropriate resource to investigate fraud.

When disagreements arise, the following Crime Allocation Escalation Procedure is followed. It is accepted that during investigation new evidence may become available which increases the seriousness or the complexity of the investigation. In such situations, it may be apparent that the investigation would be more appropriately dealt with in a different investigation level.

ROLE	ACTION REQUIRED
11.2.1 OIC (Officer in Case)	• Ensure all lines of investigation to date are detailed on the OEL. • Highlight further evidence that has increased the complexity / seriousness of the investigation. • If further offences have been disclosed, they should be recorded on RMS with appropriate supervisory management direction. • Ensure that any new safeguarding issues that have been identified are addressed.
11.2.2 Investigation Sergeant	• To discuss the case with the ECU Detective Sergeant regarding a re-triage or reallocation of the crime. • Once a decision has been made regarding reallocation, the decision maker should update the RMS OEL with the reasons for reallocation and specify who the crime has been allocated to. • In the unlikely event that the matter is not resolved the matter should be escalated to the ECU Detective inspector.

11.3 Courier Fraud

Courier fraud occurs when a suspect contacts a victim by telephone purporting to be a law enforcement official, or bank staff. The victim is persuaded to co-operate with an 'operation' designed to gather evidence or identify offenders responsible for a fictional offence. Victims are requested to withdraw money from their bank, hand over bank cards or purchase an expensive item to assist with the investigation on the promise that the money or item will be returned, or compensation provided. The money or item is then handed over to a 'courier' who attends the victim's address or meets them nearby.

Other than in very exceptional circumstances courier frauds impact on vulnerable victims. They are by their nature committed across force boundaries and are driven by organised criminality. An effective law enforcement response to courier fraud depends on collaboration across force boundaries both with other police forces and Regional partners. For this reason, oversight of all courier fraud investigations in North Wales will be undertaken by the Economic Crime Unit under the direction of the Detective Inspector. (please refer to appendix)

11.3 Romance Fraud

Romance Fraud is a high harm fraud type and can be difficult to disrupt as quite often the victim may not see themselves as a victim or may not be ready to accept that they have been deceived.

Disrupting this fraud type is an important part of our safeguarding response. The Romance fraud process map reflects our approach to utilising all sources of information to identify offences and disrupt the offence.

12. MONEY MULE PROCESS

12.1 Role of a Money Mule

Money muling is when an individual, commonly referred to as a 'money mule', moves the proceeds of crime on behalf of criminals, sometimes in exchange for payment or other benefit. Money muling allows criminals to hide their involvement in the movement of criminal property.

The money is transferred from the mule's account to the scam operator, typically in another country. Money mules are a key part of economic crime and their disruption by law enforcement is desirable to disrupt wider criminality.

Often, the mule is paid for services with a small part of the money transferred. Money mules are commonly recruited with job advertisements for "payment processing agents", "money transfer agents", "local processors", and other similar titles. The vast majority of money mules are now recruited via social media posts, and the profile of mules reflects that they are often recruited because of their own vulnerabilities.

The benefit to the criminals is not the work carried out by the mule, but that the criminals are distanced from the risky, visible transfer. Candidates are asked to accept funds and to forward them, after deducting a relatively small payment for themselves, to a third party, which they can do from home.

After money or merchandise has been stolen/subject to fraud, the criminal employs a mule to transfer the money or goods, hiding the criminal's identity and location from the victim of the crime and the authorities. By using 'clean' bank accounts the mule allows the thief to transform a reversible and traceable transaction into an irreversible and untraceable one.

Money mules are potentially complicit in the offence of money laundering. Incidents that would fit the definition of muling often come to the attention of police as a result of financial intelligence concerning the activity on a person's bank account, suspicious transactional activity at a money Transfer Agent (i.e. Western Union), or as a result of dissemination from Report Fraud that indicates the recipient account of fraudulent funds.

Our response to muling is aimed at disrupting the wider criminality. Intelligence indicating a person is involved in muling will be considered in line with our responsibility to safeguard.

Please refer to the process map in the appendix for guidance on our response to suspected money mule offending.

13. DECLARATION & LEGALITIES

13.1

In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall, the intention of this policy is to make North Wales the safest place in the UK.

13.2

In the writing of this policy cognisance has been taken of the organisation's ongoing commitment to the Code of Ethics.

13.3

North Wales Police policies will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.

13.4

The following main legal requirements have been identified within this policy:

- Equality Act 2010
- Human Rights Act 1998
- The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
- Data Protection Act 2018
- Freedom of Information Act 2000
- Health and Safety Act 1974

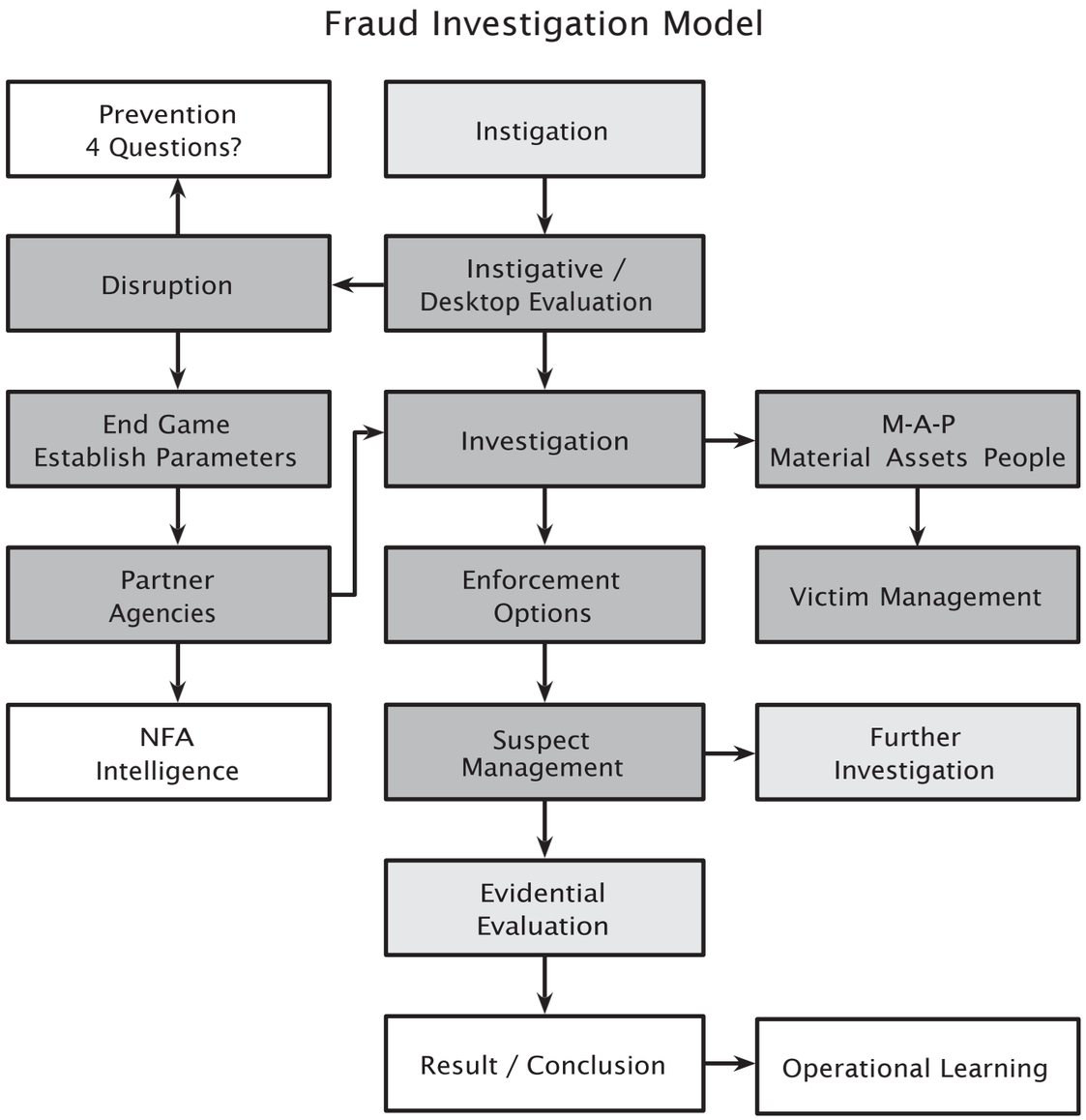
13.5

This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).

13.6

New legislative requirements or changes in Force structure may necessitate a review of this policy document.

14. APPENDIX 1 – FIM

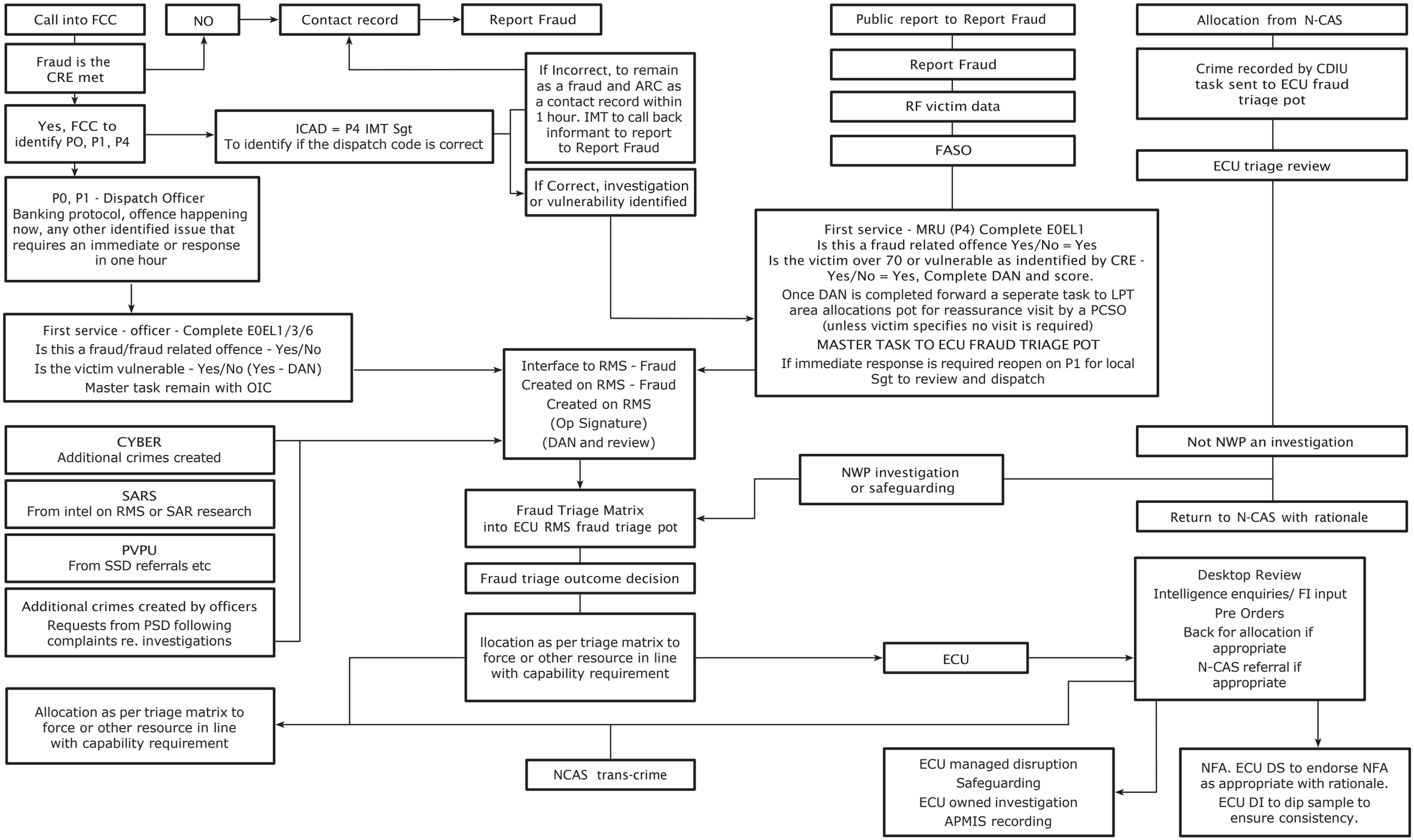


The dark grey sections represent activities requiring investigative strategies or policy decisions, the light grey sections represent the main decision points and the white sections are the outcomes that can be achieved and post investigative considerations.

15. APPENDIX 2 – FRAUD TRIAGE MATRIX

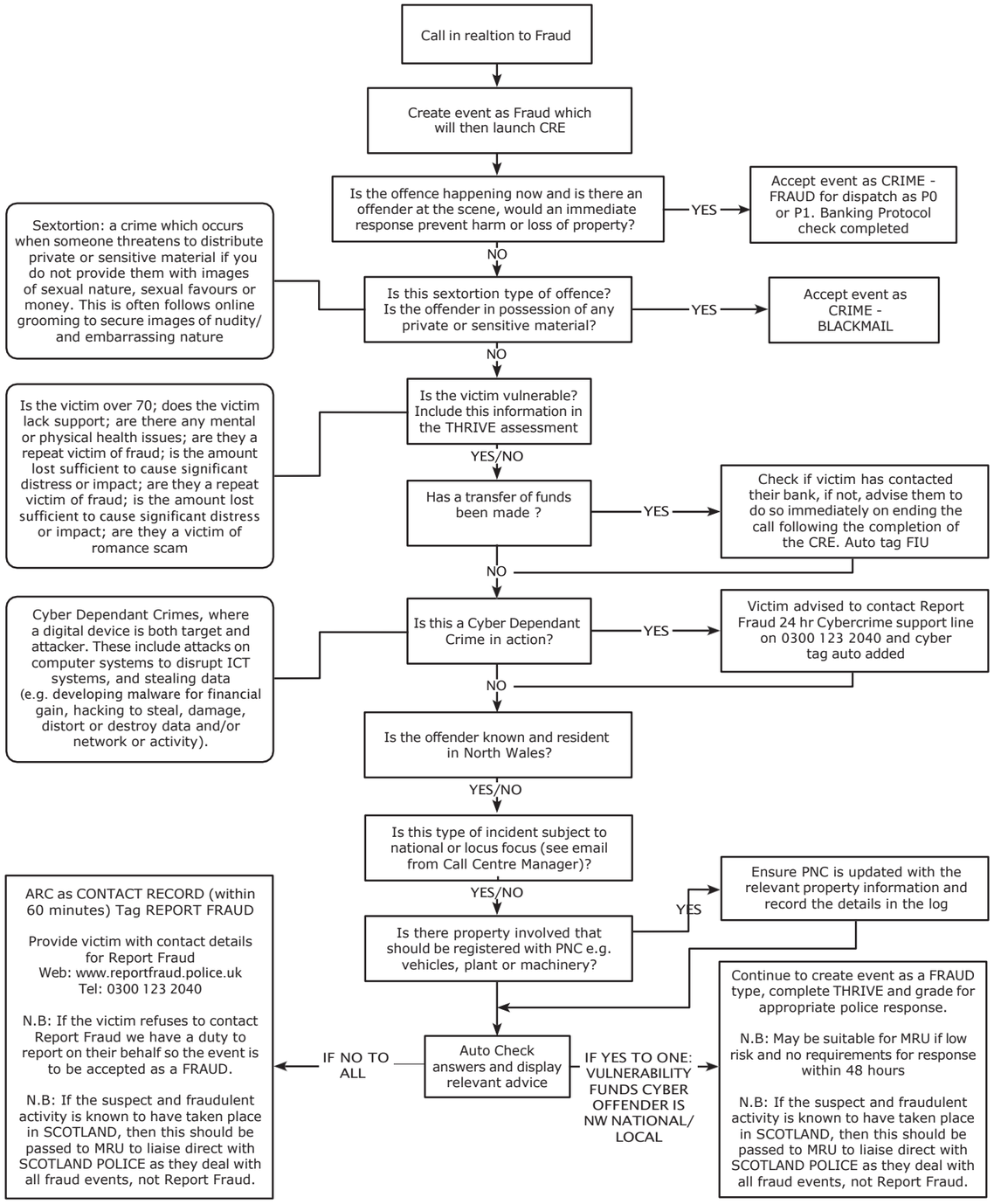
RMS Number	
Victim assessment	Please select.
Offender assessment	Please select.
Seriousness	Please select.
Resources	Please select.
Investigation	Please select.
Complexity	MINIMAL
Impact victim	Please select.
Impact business	Please select.
Opportunities	Please select.
Total score	
Allocation	Please select.
Area	Please select.
Comments	

16. APPENDIX 3 – FRAUD ALLOCATION PROCESS MAP



17. APPENDIX 4 - FCC FRAUD CRE

CRE Process Map - Workflow Fraud



18. APPENDIX 5 - COURIER FRAUD PROCESS MAP

COURIER FRAUD

WHAT IS COURIER FRAUD? Courier Fraud occurs when a suspect contacts a victim by telephone purporting to be a law enforcement official, or bank staff. The victim is persuaded to co-operate with an 'operation' which ultimately leads to the victim handing over cash or other valuables to a 'courier'.

The 'courier' may visit the victim multiple times until such time that the victim or another party recognise a fraud has taken place.

Offenders target the elderly and will target multiple victims across force boundaries making the offence difficult to detect.

A postal courier fraud is a variation of the offence where the communicator persuades the victim to post cash to an address controlled by the offender.

ACTIONS FOR THE CONTROL ROOM

An identified courier fraud should never be referred to Report Fraud, if received at FCC. Once identified the control room should allocate a resource as early as possible. Notify Economic Crime Unit during office hours.

Ensure local Pace and Ops Inspector and Supervisor are sighted on the call so that an appropriate resource can be allocated as early as possible.

FIRST RESPONDER

- Be prepared to show identification (ie. warrant card) even if you are in uniform
- Capture initial account on BWV. (How has contact been made, identify any mobile numbers, record first description of any courier)
- If their bank card has been handed over assist and encourage them to cancel their card. (An FI is not needed for this)
- Obtain description of any suspect vehicle and record any times and dates that a courier has attended.
- Consider forensic opportunities. SEEK ADVICE FROM DUTY CSI/CSM
- Identify and secure any CCTV opportunities (Ring doorbell CCTV provides excellent evidence in identifying a courier)
- Ensure victim is safeguarded and contact with the courier / victim communicator has ceased.
- Once evidence gathering is complete ensure an ICR and DAN are completed. A CID16 can also be submitted with the victim's consent.
- Notify ECU of the incident or if they are not available a CID Supervisor.
- Before you leave the premises ensure that the victim understands how the Police will contact them next. Document how this has been agreed in line with our VCOP guidelines.

INVESTIGATION

All Courier frauds in North Wales are owned and managed by ECU due to the cross border nature of the offence.
The response will be reviewed and actions allocatedby either the ECU DI or ECU FRAUD DS.
ALWAYS CONSIDER AN EVIDENCE LED PROSECUTION WITH A FOCUS ON THE DISRUPTION OF FRAUD.

COURIER FRAUD

- CCTV / H2H ENQUIRES
- COMMS DATA ENQUIRY
- REPORT FRAUD RECORD AND CROSS REF WITH NFIB
- ANPR / VEHICLE ENQUIRIES
- IF SUSPECT IDENTIFIABLE EARLY ARREST WILL DISRUPT OFFENDING AND MAXIMISE EVIDENTIAL OPPORTUNITIES. SEEK PECT SUPPORT VIA GATEWAY
- CONSIDER EARLY ABE WITH VICTIM
- ENGAGE PREVENT HUB TO PROVIDE SUPPORT

POSTAL COURIER FRAUD

- CONFIRM ALL DETAILS INCLUDING RECIPIENT ADDRESS HAVE BEEN OBTAINED
- CONFIRM VICTIM COMMUNICATOR NUMBER USED OR IF NOT AVAILABLE THE NUMBER VICTIM WAS CALLED ON
- FASO TO ENSURE TARGET HARDENING HAS BEEN CONSIDERED TO PREVENT FURTHER LOSS
- REPORT FRAUD RECORD TO BE COMPLETED AND NFIB TO REVIEW AND DISSEMINATE

REMEMBER: Courier Fraud is a crime that predominately impacts older vulnerable people. The nature of the offence will impact on how they relate to all people in Authority such as Police, Medical Staff and other persons in Authority. Our response to this offence type must at all times be focused on maintaining their trust in us as an organisation.

19. APPENDIX 6 – FRAUD DIP SAMPLING AND REVIEW PROCESS MAP

NORTH WALES POLICE CURRENTLY MANAGE FRAUD VIA A TRIAGE AND ALLOCATION PROCESS

All potential fraud investigations are reviewed via fraud triage and allocated based on complexity to either a PIP1 or PIP2 resource to investigate. This triage accounts for all fraud not just those disseminated via the portal. It is acknowledged that all investigations have competing demands and therefore fraud investigations will benefit from periodic reviews by a subject matter expert with a view To achieving a resolution at the earliest opportunity. This process highlights how these reviews are managed.

ECU TRIAGE REVIEW FRAUD REPORT AND DETERMINE WHETHER OR NOT NWP WILL INVESTIGATE IN ACCORDANCE WITH THE FRAUD POLICY OCCURRENCE ENDORSED APPROPRIATELY WITH RATIONALE AND INVESTIGATION STRATEGY REPORT FRAUD UPDATED

ECU ALLOCATION

Investigation triaged and allocated to appropriate resource endorsed with rationale and investigative strategy. Ownership of investigation transferred to the relevant team.

6 MONTHS

ECU FRAUD supervisor will dip sample 5-10 fraud investigations each month to ensure the investigation strategy is being followed and to keep the case on track.

12 MONTHS

ECU DI to dip sample 10 cases that have passed this point and help address issues preventing progression.

ECU NFA

Investigation reviewed by triage officer. Decision made and complainant update.

FRAUD DS

Review all fraud cases that are not progressed at triage stage, confirm decision, endorse and close.

ECU DI

Dip sample 5 NFA cases per month to ensure that decisions are appropriate and in line with force policy.

- Trends identified during dip sampling will be reported back to the investigation standards board so that any consistent issues or good practice can be highlighted for wider learning
- All dip sampled cases will be endorsed with the appropriate template to document that a review has taken place and to provide any required further guidance to the investigator.
- The ECU DI will keep a record of all cases dip sampled.

20. APPENDIX 7 – MONEY MULE PROCESS MAP

MONEY MULE PROCESS MAP

MONEY MULE: Money muling is when an individual, commonly referred to as a 'money mule', moves the proceeds of crime on behalf of criminals, sometimes in exchange for payment or other benefit. Money muling allows criminals to hide their involvement in the movement of criminal property. Money muling is illegal but frequently those involved have vulnerabilities which facilitate their exploitation. This map allows for a consistent approach in terms of our response to this issue.

FASO

Identify evidence of money muling via safeguarding referrals and other incoming information.

FINANCIAL INTELLIGENCE OFFICER

Identify evidence of money muling via SAR research in line with agreed keyword searches. Sanitise and record intelligence on NWP systems.

SAFEGUARDING

Prioritise the safeguarding of the individual. Complete all relevant checks that may assist in determining whether the individual is being exploited and document research accordingly. Update ECU Supervisor for assessment and classification.

SAFEGUARDING ONLY

- Vulnerable Victim Notice as appropriate
- Safeguarding referral (CID 16)
- Further visit to subject gather more evidence of recruitment, exploitation.
- Record and share intelligence
- APMIS record as appropriate
- Consider further disruption opportunities.

SUSPECT

- ECU FINANCIAL to assist with intel package (inc Open Source requests)
- DS to review package and allocate to appropriate resource with recommended action
- Suspect to be processed via Cease and Desist or Money Laundering investigation.

REVIEW

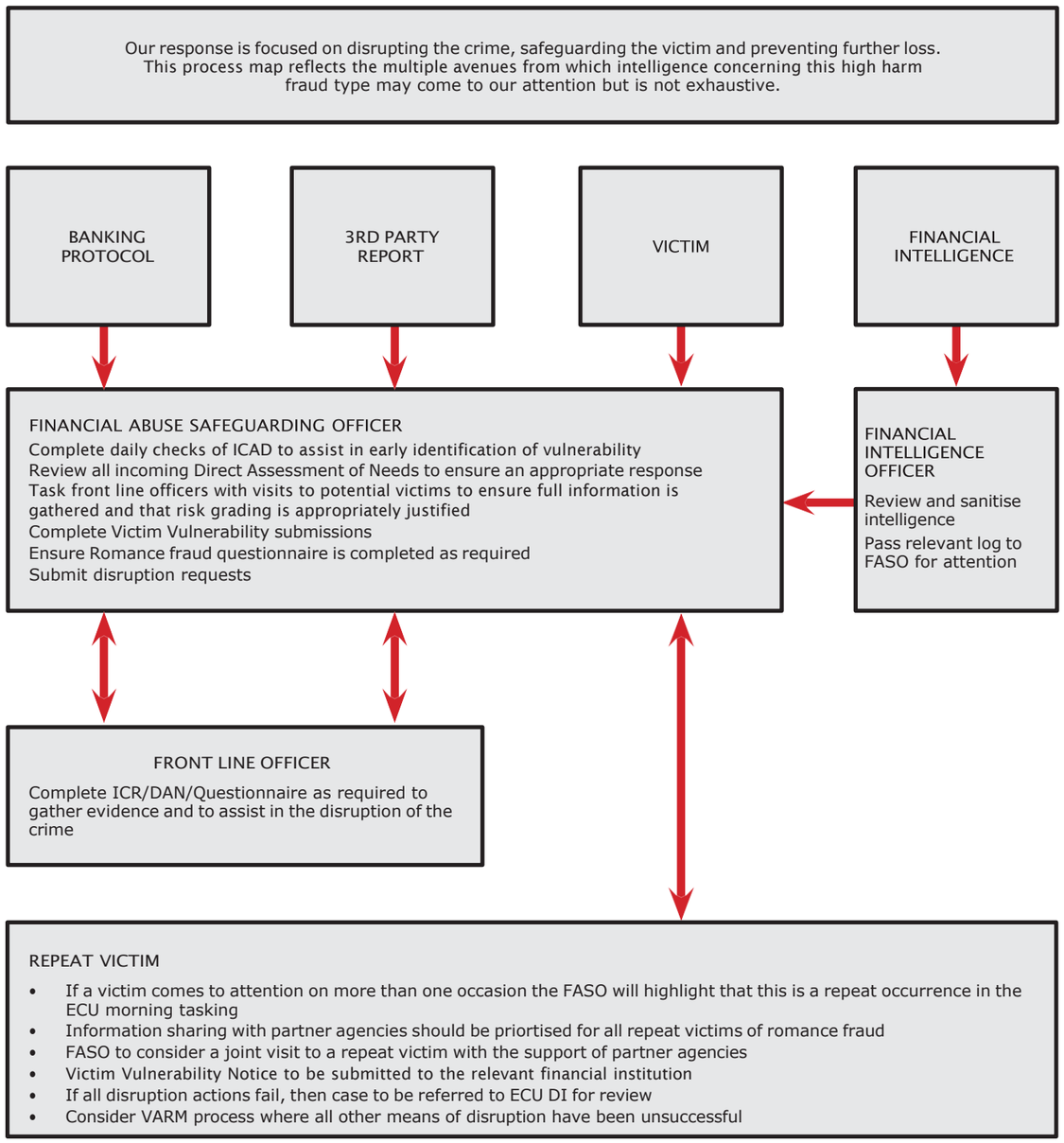
On review of fresh information subject to be further reviewed and resubmitted to DS for consideration of further action.

OUTCOME

- Outcomes to be recorded in line HOCR guidelines,.
- Cease and Desist to be recorded as Outcome 22.

21. APPENDIX 8 - ROMANCE FRAUD PROCESS MAP

ROMANCE FRAUD PROCESS MAP



22. APPENDIX 9 – CODE FOR CROWN PROSECUTORS

Code for Crown Prosecutors Para 4.12 a-g:
The key points are as follows:

How serious is the offence committed?

The more serious the offence, the more likely it is that a full investigation is required.

What is the level of culpability of the suspect?

Regard should be given to considering culpability as to whether the suspect is, or was at the time of the offence, suffering from any significant mental or physical ill health as in some circumstances this may mean that it is less likely that an investigation is required.

What are the circumstances of, and the harm caused to the victim?

The circumstances of the victim are highly relevant. The greater the vulnerability of the victim, the more likely it is that further investigation is required. This includes where a position of trust or authority exists between the suspect and victim.

An investigation is also more likely if the offence has been committed against a victim who was at the time a person serving the public.

Regard must be given as to whether the offence was motivated by any form of discrimination against the victim's ethnic or national origin, gender, disability, age, religion or belief, sexual orientation or gender identity; or the suspect demonstrated hostility towards the victim based on any of those characteristics. The presence of any such motivation or hostility will mean that an investigation is required.

In deciding whether an investigation is required in the public interest, any decision should take into account the views expressed by the victim about the impact that the offence has had. In appropriate cases, this may also include the views of the victim's family.

Consideration should be given as to whether an investigation is likely to have an adverse effect on the victim's physical or mental health, always bearing in mind the seriousness of the offence. If there is evidence that any subsequent prosecution is likely to have an adverse impact on the victim's health it may make further investigation less likely, taking into account the victim's views.

Was the suspect under the age of 18 at the time of the offence?

The criminal justice system treats children and young people differently from adults and significant weight must be attached to the age of the suspect if they are a child or young person under 18. The best interests and welfare of the child or young person must be considered including whether any potential prosecution is likely to have an adverse impact on his or her future prospects that is disproportionate to the seriousness of the offending.

What is the impact on the community?

The greater the impact of the offending on the community, the more likely it is that further investigation is required.

APPENDICES

- Fraud Investigation Model
- Triage Matrix
- Process Allocation Process Map
- Force Control Centre CRE Map
- Courier Fraud Process Map
- Dip Sampling and Review Process Map
- Money Mule Process Map
- Romance Fraud Process Map
- Code for Crown Prosecutors (Para 4.12 a-g)

HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

92768.