HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

Response Date:16/06/2026

2026/624 - Fraud Policy and case files

In response to your recent request for information regarding;

I am aware that N Wales Police have stated to me they have a policy that fraud over two years old will not be investigated despite the effect this has on victims. I note the case against R Hallows was heard in Court in 2023 and yet the fraud occurred in 2014-2018.

A Fraud Policy wasn't created in Force until 2018, please find attached the version used from 2018 – 2020 and our current policy.

In addition to the files which affected me and as there is a close interest in the others defrauded by R Hallows I would ask for the full details of the case files against R Hallows which resulted in his conviction and imprisonment in 2023.

The information you have requested constitutes personal data of which you are not the subject and disclosure of the information to a member of the public otherwise than under the Data protection Act 2018 would contravene the data protection principles.

Section 40 is a class based exemption, therefore it is not necessary to evidence harm caused by disclosure.

The data protection rights of a third party would be breached by disclosure, therefore section 40(2) is an absolute exemption and a Public Interest Test is not necessary. This is so because personal data is governed by another law (The Data Protection Act 2018) and there are two elements to this exemption.

All requests made under FOIA are applicant blind. A request must be treated as such and a public authority will always view any disclosure as into the public domain. Thus North Wales Police must be satisfied that any release of information will be potentially available to the general public. It is therefore on this basis that the following is relevant.

The first element of this exemption is engaged if the information requested constitutes personal data and is made by the data subject. The information will be covered by section 40(1) and the request will be dealt with under the Data Protection Act, rights of access.

The second element of this exemption is engaged if the personal data is about someone other than the applicant. Where someone makes an application for information other than the data subject, disclosure of that information will often constitute a breach of the Data Protection Act covered by section 40(2).

Personal data is regulated under the principles of the Data Protection Act and when information contains personal data about a third party it can only be refused if disclosure would breach any of the data protection principles.

As previously highlighted, any disclosure under the FOIA is a public disclosure and release of the identity of an individual would breach principles 1 & 2 of the Data protection Act 2018.

These principles require that: 1) the processing of personal data for any of the law enforcement purposes must be lawful and fair and 2) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate.

'Data subjects' are provided with certain legal enforceable rights under the Data Protection Act 2018. The fact that the information is held for lawful policing purposes, disclosing it onwards would breach the principles, and would be incompatible with the data subject's right that their data is held securely. By disclosing this information, the force could be subject to enforcement proceedings under the act if it breaches any of those principles.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 12/06/2026

HEDDLU GOGLEDD CYMRU
Gogledd Cymru diogelach

NORTH WALES POLICE
A safer North Wales

Fraud Policy

Governance:	**Operations Committee**		
Policy Owner:	**DCI Fraud Lead**		
Department:	**Local Policing Services**		
Policy Writer:	**LPS Fraud Lead**		
Policy Number:	**151**	**Version:**	**1.0**
Effective Date:	**12/12/2018**		
Review Date:	**12/12/2020**		

CHANGE HISTORY

Version No:	Author	Changes	Ratification
1.0	…		

Contents

1. WHY IS THIS POLICY REQUIRED?

This policy

1.1 Seeks to protect the communities of North Wales who are at risk as a result of fraud.

1.2 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.

1.3 Sets out the agreed model for allocating and investigating volume and major fraud offences.

1.4 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.

1.5 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.

1.6 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.

1.7 Provides clear and consistent standards to ensure the effective supervision, management and prioritisation of fraud investigations.

1.8 Adopts a proactive multiagency approach in preventing and reducing fraud.

2. WHO SHOULD USE THIS POLICY?

2.1 This policy should be used by all North Wales Police Officers and staff. Individual managers and supervisors are responsible for ensuring that this policy is applied in their area of operations.

2.2 This policy includes:

- An outline of the role of the **Financial Abuse Safeguarding Officer (FASO)** in assessing and protecting vulnerable victims of fraud
- The **Direct Assessment of Need (DAN)** process (see Appendix 1) to ensure that vulnerable victims are correctly identified and supported
- An outline of the agreed National Fraud Reporting process whereby North Wales Police will direct any person wishing to report a fraud to the **Action Fraud** contact centre unless the case meets the agreed call for service criteria
- The principles on which frauds will be triaged
- 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
- A requirement to follow the National **Fraud Investigation Model** (See Appendix 2) for relevant fraud investigations

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

3.1 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.

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

- National Fraud Strategy
- City of London Police Cyber Crime Key Assessment for North Wales Police
- City of London Police Fraud Profile for North Wales Police
- The Little Book of Big Scams

4. ROLES & RESPONSIBILITIES

4.1 Force Control Room	• Follow the agreed National Fraud Reporting process whereby North Wales Police will direct any person wishing to report a fraud to the Action Fraud contact centre unless the case meets the agreed call for service criteria
4.2 Any Officer receiving a report of a fraud	• Follow the agreed National Fraud Reporting process whereby North Wales Police will direct any person wishing to report a fraud to the Action Fraud contact centre unless the case meets the agreed call for service criteria
4.3 FASO (Financial Abuse Safeguarding Officer)	• Assess and protect vulnerable victims of fraud • Supporting area with the triaging and allocation of fraud cases • Provide advice and assistance to Initial Investigating Officers/ Supervisors
4.4 NWP Investigation Support Team	• Receive all fraud investigations from Action Fraud and create occurrences. • Follow the National **Fraud Investigation Model** (see Appendix 2)
4.5 Fraud SPOC's Within District CID	• Provide advice and assistance to Initial Investigating Officers/ Supervisors • Triaging and allocation of fraud cases received from Action Fraud
4.6 FCR (Force Crime Registrar)	• Review and ratify applications of outcome 21 ensuring the highest standards of integrity and victim focus.

4.7	**Managers/ Supervisors**	• Ensure this policy is applied in your area of operations.

5. THE FRAUD REPORTING PROCESS

5.1 Reporting Fraud Offence - Action Fraud

Action 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.

A vulnerability assessment should be undertaken by the Force Control Room in any case where a victim is reporting fraud prior to advising the victim to report the matter to Action Fraud.

5.2 Vulnerability Assessment

Role	Action Required
5.2.1 **Force Control Room/ Any Officer receiving a report of a fraud**	• Undertake a **Vulnerability Assessment** where a victim is reporting fraud ***prior*** to advising them to report the matter to **Action Fraud**. • follow the **CRE Process for fraud** • See sections 5.3 & 5.4 below
5.2.2 **Initial Investigating Officer & Supervisors**	*Please note*: North Wales Police will follow the National **Fraud Investigation Model** (see Appendix 2) • Consider if the person reporting should be referred to their bank/financial institution and/or Action Fraud. If the person reporting is vulnerable or the case meets the 'call for service' criteria you should then: • 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 fraud SPOC's within District CID, Financial Investigation Unit (FIU) or Financial Abuse Safeguarding Officer (FASO). • Report the details of the crime to **Action Fraud** in accordance with **NCRS** (National Crime Recording Statistics). • Record the NFRC number (the national crime number) in the OEL of the Niche occurrence. • Do **NOT** submit the crime for filing *until* an NFRC is obtained and placed on the OEL. If the victim is unable to report the matter to Action fraud the initial responder should assist or complete the report on behalf of the victim

5.3 Offences not recorded by Action Fraud

Do **NOT** report the following fraud offences to Action Fraud

- If a report of fraud requires either immediate police action **or** involves a vulnerable victim
- making, supplying or use of articles to commit fraud*

- possessing/controlling article(s) for use in fraud*
- possession of false documents*
- theft of fuel*
- forgery or use of drug prescription*
- fraud or forgery relating to vehicle or driver records*
- other forgery*

  (***** these are ***not*** recorded by Action Fraud)

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

All other reports of fraud (including Live Cyberattacks) should be made to **Action Fraud** via their website www.actionfraud.police.uk or by telephoning **0300 123 2040**. (For more details, see Flow Diagram on page 6)

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

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

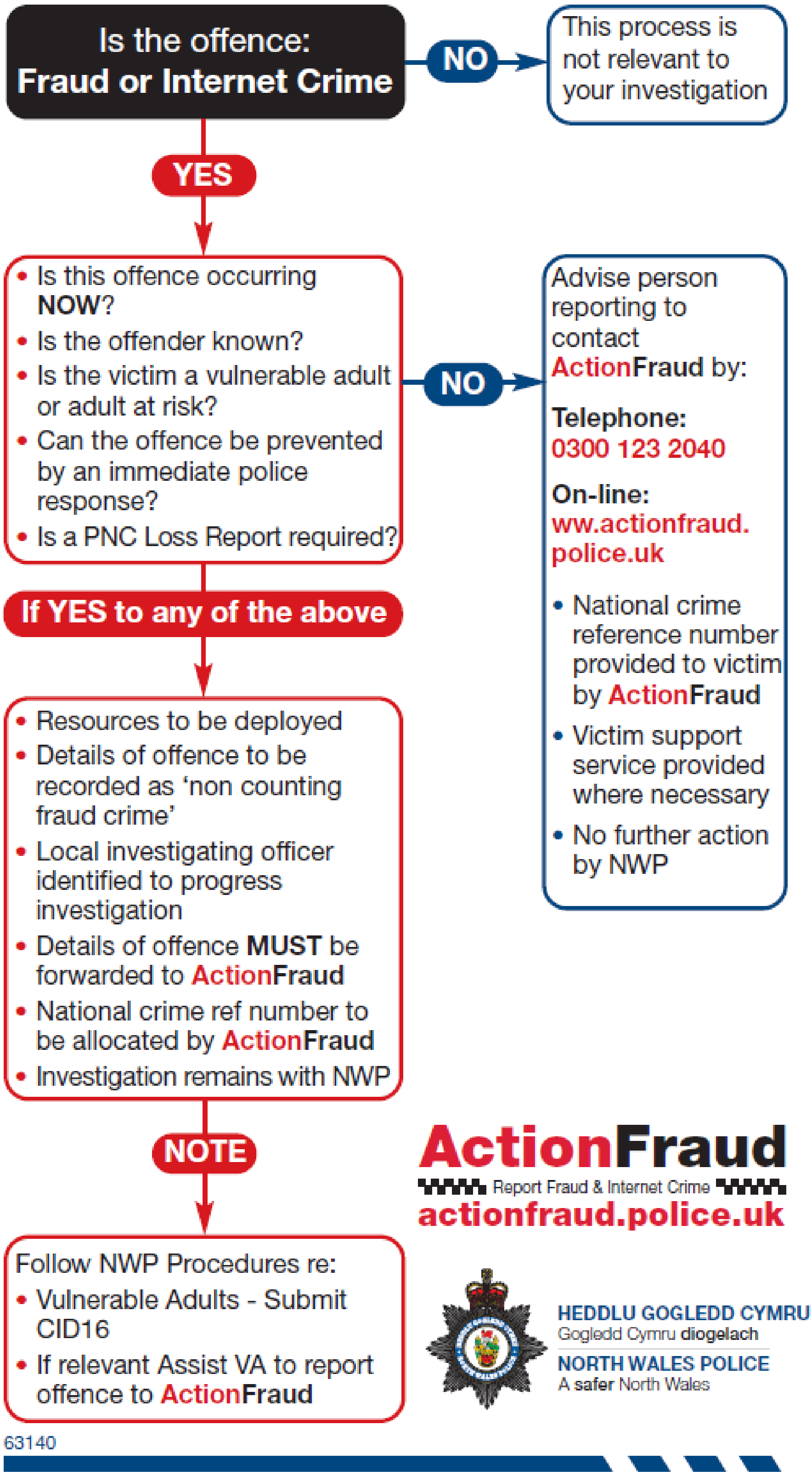
Before referring to Action Fraud

5.5 Role of IST in Recording Fraud Occurrences

All fraud investigations received directly from Action Fraud will be forwarded to the North Wales Police IST department and an occurrence created. Thereafter they will be tasked to the respective Local Policing Area Detective Chief Inspector and Financial Abuse Safeguarding Officer (FASO) for triaging and allocation (if required).

All Transfer of Crime / Cancellation requests in relation to NFIB (Action Fraud) recorded fraud must be submitted to the Deputy Crime Registrar requesting transfer.

5.6 Fraud Reporting Process Flowchart



6. VULNERABILITY ASSESSMENT FOR VICTIMS OF FRAUD

6.1 In accordance with Action Fraud's Crime Allocation principles, 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.

6.2 To safeguard victims of fraud in North Wales, the FASO assesses all North Wales victims of fraud crimes for repeat victimisation and/or vulnerability.

6.3 The Vulnerability Review

Role	Action Required
6.3.1 **FASO**	• Initially review the Action Fraud data • Prioritise it into the following six categories: 1. Aged 70+ 2. Aged 60-69 years 3. Other victims who identify to Action Fraud that they have been significantly affected by what happened (Aged 0 – 59) 4. Aged 0-59 5. Organisation 6. No Date of birth listed • Also review The Action Fraud data to identify repeat victims (including repeat businesses).

6.4 All victims aged 70 and over

Role	Action Required
6.4.1 **Force Control Room / Any Officer received a report of fraud**	• The Force Control Room Staff will follow the Customer Rules Engine for Fraud reports. • 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.
6.4.2 **PCSO/ Police Officer**	• Complete Direct Assessment of Needs questionnaire (DAN) • Place the DAN on RMS • Provide Crime Prevention advice on that visit to prevent repeat victimisation.
6.4.3 **FASO**	• Review the Direct Assessment of Needs using **Operation Signature Risk Assessment Template** (see Appendix 3). • Place on the OEL an outline of any additional safeguarding or support that is required from the Safer Neighbourhood Team. This occurrence is then re-tasked back to the PCSO or Police Officer who completed the initial DAN or to the relevant crime allocations pot for the area concerned for allocation if required. • Actively monitor tasks that have been sent to the respective allocations pots within NICHE.

	• Once they are completed, risk assess the victim using the Operation Signature Risk Assessment Scoring Model to identify any further needs. • Complete referrals to Victim Help Centre • Consider disruption action to protect victim(s)

6.5 <u>Victims Aged under 70</u>

These victims may also receive a personal visit if they are:

- a repeat victim
- or from the information provided they are identified as vulnerable

Role	Action Required
6.5.1 **FASO**	• Provide crime prevention advice by email (if email address is available) along with your contact details so that victims can make contact with the FASO if they require any additional advice or support. • Examine data within the Action Fraud data to establish websites, email addresses and telephone numbers of the suspects for purposes of disruption. • If the victim has been using Money Service Bureau's (MSB's) to transfer money to suspects the FASO will consider making contact with SPOC's within those MSB's to have their accounts temporarily suspended to prevent further offences. • Monitor all events of 'Banking Protocol' to ensure that the Banking Protocol is being complied with. • Share the information with the relevant trading standards departments if applicable. • In the event of any breaches of Banking Protocol contact the coordinator at UK Finance. • Share the Banking Protocol returns with the Cyber Protection Officer at the City of London Police on a ***monthly*** basis.

6.6 <u>Victim identified as High Risk</u>

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.

6.7 This Fraud Triage 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.

6.8 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 Triage principle categorises each case into one of the below:

CAT 1	**Must** be investigated by North Wales Police either alone or in partnership with an enforcement agency (DWP, Trading Standards, HMRC, Pensions Regulator, Charities Commission etc.)
CAT 2	Following triage and some initial enquiries, it is apparent that the offender does not reside in North Wales and therefore would be more appropriately investigated by another force.
CAT 3	Cross border offenders or of such complexity that consideration should be given to referral through to Titan, NCA or SFO.
CAT 4	Due to the specific nature of the fraud, would be more appropriately investigated led by a partner agency (DWP, Trading Standards, HMRC, Pensions Regulator, Charities Commission etc.).
CAT 5	Where disruption would be the most beneficial course of action either alone or in conjunction with a partner agency (DWP, Trading Standards, HMRC, Pensions Regulator, Charities Commission etc.)
CAT 6	Should be sign-posted to civil procedures.
CAT 7	Should not be investigated, as these cases are not considered to be within the public interest.

8. PRIORITISATION OF INVESTIGATION

8.1 Prioritisation of Investigations – High Priority Cases (Consider CAT 1-5 only)

- 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 - Lower Priority Cases (All Categories)

- The investigation would require a disproportionate level of resources to bring the case to a conclusion and would adversely impact upon our ability to investigate other crimes.

- The victims 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 has repaid the victim and the bank/financial institution is not pursuing a complaint.

- 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 victim has pursued civil recourse and has subsequently turned to the police for a criminal investigation as a result of dissatisfaction with the civil remedy.

- Delays to the investigation will be caused by the location of key evidence elsewhere.

- Victims have ignored guidelines that are designed to prevent them becoming victims of fraud, for example, online banking and auction sites.

- Frauds where the victim's conduct has contributed to the loss, in particular, where the police have previously given guidance or warnings to victims about fraud risks that have not been acted upon.
- Cases where the victim's motive for making the complaint appears to be malicious and is primarily focused on recovering monies owed, or designed to distract attention from the complainant's own involvement in the fraud. (Such cases might

nevertheless merit investigation, particularly where there are other victims involved).

- Cases where victims are not prepared to co-operate fully with the investigation and prosecution, although we will always consider carefully how to assist victims and witnesses who have concerns about safety.

- Frauds more suitable for investigation by another enforcement or regulatory agency.

- Cases where another police force has decided not to investigate other than for geographical reasons.

- Frauds that have already been investigated by the police or another enforcement agency, or that have been the subject of regulatory proceedings, unless significant new evidence has come to light or the previous investigation had a narrow remit that did not address all the relevant issues.

- Cases where the existence of other proceedings might have a detrimental effect on a criminal investigation and subsequent prosecution.

- Frauds which took place a long time ago (probably more than 2 years), unless there are exceptional circumstances.

Fraud Triage will give due consideration to the Category and Priority of each case using the indicators. A decision is then made to allocate to either:
• a Patrol Officer
• a CID Officer
• a Cyber Crime Team Officer
• to set up a dedicated investigation team
• or to consider <u>no investigation</u> or <u>alternative resolutions</u>

9. NO INVESTIGATION

9.1 If the decision is to ***<u>not</u>*** investigate: -

- 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 <u>Appendix 4</u>) which must be authorised by a Detective Sergeant or above with the rationale for issue endorsed on the occurrence.

- **outcome type 21** is to be used to file the case on RMS and NFIB advised.

9.2 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 <u>not</u> 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 Registrar (FCR) 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 *<u>must</u>* be informed of the decision in writing.

Role	Action Required
9.2.1 **Force Crime Registrar**	• Periodically review the application of outcome 21 to ensure the highest standards of integrity and victim focus. • Refer unsuitable cases to the respective Divisional Crime Manager for further consideration for a full investigation.

Standards of outcome 21 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.

9.3 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. All such cases must be referred to the Divisional Crime Manager for authorisation ***before*** the victim is informed of the outcome.

9.4 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 5.

10. ALTERNATIVE RESOLUTION FOR FRAUD

10.1 As above reference is made to disruption, joint agency working and civil resolution (**CAT 4/5/6** specifically). 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 and must be used in conjunction with the Category and Priority sections 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.

10.2 Cyber Enabled Fraud

Type of Fraud	Potential Alternatives to investigation may include the following:
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	• **Criminality notice to offender** • **Refer to Trading Standards to use bespoke powers if they wish to proceed** • **Submit intelligence accordingly on Niche**

materialise using the internet or telephony.	• **Advise victim 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.**
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 (noting the offenders are mainly abroad).**
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.	• **Criminality notice to offender** • **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.**
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.**
Intellectual Property Fraud This is when fake goods are passed off as originals and effects many industries including health, music, film, fashion and fragrances.	• **Refer to Trading Standards** • **Refer to the Intellectual Property Office** • **Refer to FACT (Federation Against Copyright Theft) if music or film**

	related offences
Domain Name Scams This scam is offering businesses first refusal on a domain name, suggesting someone else is just about to buy it or by sending out bogus domain name renewal notices.	• **Criminality notice to offender** • **Submit intelligence accordingly on niche** • **Advise victims by letter of outcome and offer crime prevention advice** • **Refer to Nominet to consider whether abusive registration**

10.3 Mass Marketing and Miscellaneous Fraud

Type of Fraud	Potential Alternatives to investigation may include the following:
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.	• **Criminality notice to offender** • **Refer to Trading Standards to use bespoke powers if they wish to proceed** • **Submit intelligence accordingly on niche** • **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.**
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 (noting the offenders are mainly abroad).**
Mandate Fraud This type of fraud is when someone gets a	• **Criminality notice to offender** • **Submit intelligence accordingly on**

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.	**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.**
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** • **Criminality notice to offender** • **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 visit 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**
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)** • **Criminality notice to offender** • **Submit intelligence accordingly on RMS** • **Advise victim of the outcome**

Mail Scams Legitimate mail boxes and post redirections can be used in the application of fraud.	• **Criminality notice to offender** • **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.	• **Criminality notice to offender** • **Intelligence to be submitted accordingly on niche** • **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.**
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 visit to business premises with Trading Standards and DWP and criminality notices served** • **Intelligence to be submitted accordingly on RMS** • **Victims to be advised of the outcome and crime prevention advice offered**

10.4 Investment and Banking Fraud

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.	• **Criminality notice to offender** • **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**
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.	• **Criminality notice to offender** • **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.**
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 these organisations will not undertake an investigation, • **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**

10.5 **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. As such FIU should be notified so a POCA asset review can be undertaken and an investigation strategy formulated.

Role	Action Required
10.5.1Triaging Officer	• Justify this decision • Provide guidance and advice to investigators in relation to points to prove alongside the relevant investigation strategy.

11. FRAUD INVESTIGATION PROCEDURES

11.1 Action Fraud 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.*

11.2 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 Action Fraud and if not challenge it through the Action Fraud Spoc namely the Deputy Crime Registrar.

11.3 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 by the divisional Single Point of Contact.

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

- Patrol Officer
- a CID Officer
- a Cyber Crime Team officer
- to set up a dedicated investigation team
- or to consider no investigation or alternative resolutions

11.5 Exceptions

11.5.1 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). Such cases will be retained/ referred to the appropriate PVPU so that threat, harm and risk can be addressed via mainstream safeguarding procedures.

11.5.2 Due to the structures of the national Action Fraud and NFIB, all Cyber Dependent offences received by Action Fraud are processed by NFIB 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 (Bitcoin) in return for release of their computer system. Allocation of these cases is decided following consultation with the Divisional Crime Manager, Cyber Crime Manager and FIU Manager.

11.6 Escalation

11.6.1 As per the Crime Allocation Procedure, a common sense approach is taken regarding allocation of viable fraud investigations. Building effective, collaborative relationships between the Cyber Crime Unit, FIU, Patrol Officers and divisional CID Teams is key to ensuring open discussions in the interest of the victim and our community to determine the most appropriate resource to investigate fraud.

11.6.2 When disagreements arise, the following Crime Allocation Escalation Procedure is followed. It is accepted that during an 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
11.6.3 **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.
11.6.4 **Investigation Sergeant**	• Discuss the case with the local area detective sergeant regarding the 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 a DI.

12. MONEY MULE PROCEDURE

12.1 Role of a Money Mule

A money mule (sometimes called a "smurfer") is a person who transfers money acquired illegally (e.g., stolen, obtained through fraud) in person, through a courier service, or electronically, on behalf of others. The money is transferred from the mule's account to the scam operator, typically in another country.

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. Some money mules are recruited via dating sites/romance scams.

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 true identity and location from the victim of the crime and the authorities. By using instant payment mechanisms such as Western Union, 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 Action Fraud that indicates the recipient account of fraudulent funds.

Depending on the circumstances and nature of the report/intelligence, there may be a clear suggestion that the person involved is in fact highly vulnerable and as much a victim themselves as well as being complicit in the transfer of potential criminal monies (e.g., as part of a dating/romance fraud).

12.2 The 3 stage process for the escalation of police intervention in such circumstances

Stage 1 **At this triage stage, it is likely the incident will have been allocated for a safeguarding visit.**	**The Officer/PCSO** • Serve a warning letter on them outlining that they are potentially laundering the proceeds of crime and must stop. • Complete a proforma statement detailing that this warning has been given. • Update the Op Signature safeguarding “non-counting” Niche Occurrence. Safeguarding should still be considered for the victim and any other person identified sending monies. This is also to be recorded on the incident. If the (Muling) activity continues: If the victim continues to receive and send monies after initial police intervention, the offence of money laundering under S327 Proceeds of Crime Act (convert/transfer criminal property) is potentially made out. The rationale being that the subject should have “known or suspected” the proceeds are derived from crime because an attending officer has previously advised them so.
Stage 2 **The occurrence will be assessed and allocated as**	• A separate Niche Crime Occurrence will be created for the offence of Money Laundering. The victim will now be recorded as a suspect of

per force policy to an officer to investigate.	that offence and following initial enquiries (where possible) invited for Voluntary Attendance/interviewed under caution bearing in mind any identified vulnerabilities. Once an account has been gained from the suspect a decision can be made as to the scope of any investigation and likely outcome. Given the nature of the vulnerabilities identified by the **Op Signature process** (see Appendix 3), on the first occasion a suspect is interviewed/investigated it is highly possible that a decision will be made that the matter is not suitable for prosecution/NFA (consider HO Outcome 10, 15, 16 or 21). However, the process of conducting a formal, recorded interview under caution allows police to capture the suspect "knowledge or suspicion" in an evidential format. Suspects should be advised as part of the interview process that the record of interview may be used in future proceedings should the activity continue. Consideration should also be given to the service of a Cease & Desist letter at this time.
Stage 3 **In those cases where, after previous intervention a suspect persistently continues to engage in muling activity**	• A separate Niche Crime Occurrence (Money Laundering) will be created again. If necessary or appropriate the suspect will be arrested or invited for Voluntary Attendance/interviewed under caution, and a file submitted to CPS if appropriate. Following advice from the CPS, it is recommended that consideration be given to exploring the use of CBO`s post-conviction, or SCPO`s (which are available on a standalone civil basis) as an alternative method of disposal, or means of controlling muling behaviour.

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 provide a safer North Wales.

13.2 In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014).

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 Measure (Wales) 2011 and the Welsh Language standards
- Data Protection Act 2018
- Freedom of Information Act 2000
- Health and Safety Act 1974
- Race Relations (Amendment) Act 2000
- Policing Bureaucracy Gateway

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).

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

APPENDIX 1 – Direct Assessment of Need (DAN) Form

Name		Date of birth	
Address			
Telephone		Mobile	

Email address					
Attendance date		Attending officer		RM/RC	

Did the victim initially report the fraud to the police ?	Yes/No
Was the victim advised to contact Action fraud ?	Yes/No

How has the victim been contacted	Phone	
	Email	
	Post/Mail (Consider seizing mail)	
	In person (door step)	
	Other	

How frequent has contact been made ?									
Daily		Weekly		Fortnightly		Occasionally		Never	

Has the victim sent any money ?	Yes/No

Under £100		£100 - £1000		£1000 – £10,000		Over £10,000	

How frequent has money been sent ?									
Daily		Weekly		Fortnightly		Occasionally		Never	

How has the victim sent money – tick as many as appropriate											
Cheque		Cash		Bank card		Money transfer		Postal order		Other	

Provide details of suspect: Names provided, account numbers, sent cheque numbers, postal orders, recipient addresses, e mail addresses, reference numbers of MSB (money service businesses)

When did the activity start?									
Under a year		1-2 Years		2-5 years		5-10 years		Over 10 years	

What (if anything) triggered this activity? (e.g. death of a spouse)
Provide details of the victim's bank account (if they have been transferring from that account).

How affected are they by what has happened to them?							
Affected a great deal		Moderately affected		Affected a little		Not affected	

Do they have a support network? Family, friends, neighbours? What social interaction do they have?	Yes/No - Specify

What type of fraud/scam has/is taking place							
Dating/romance Health, medical		Lottery/Prize draws		Investment Inheritance		Computer software	

Door to door Rouge trader		Catalogue		Clairvoyant's		Courier/Telephone	

Are there any other vulnerabilities evident: Does the victim feel threatened, intimidated, frightened, and isolated? Pregnant, hoarder, victim of any other fraud type offences, cold callers, rouge traders other doorstep crime. Do they have any children/dependants?	Yes/No

Do they have any health issues? Consider: Physical, Mental health Visual/speech/hearing impairment mobility	Yes/No - Specify		
Do they live alone?	Yes/No	Are they recently widowed/separated	Yes/No
Does the victim have any home care support	Yes/No	Company name & telephone number	

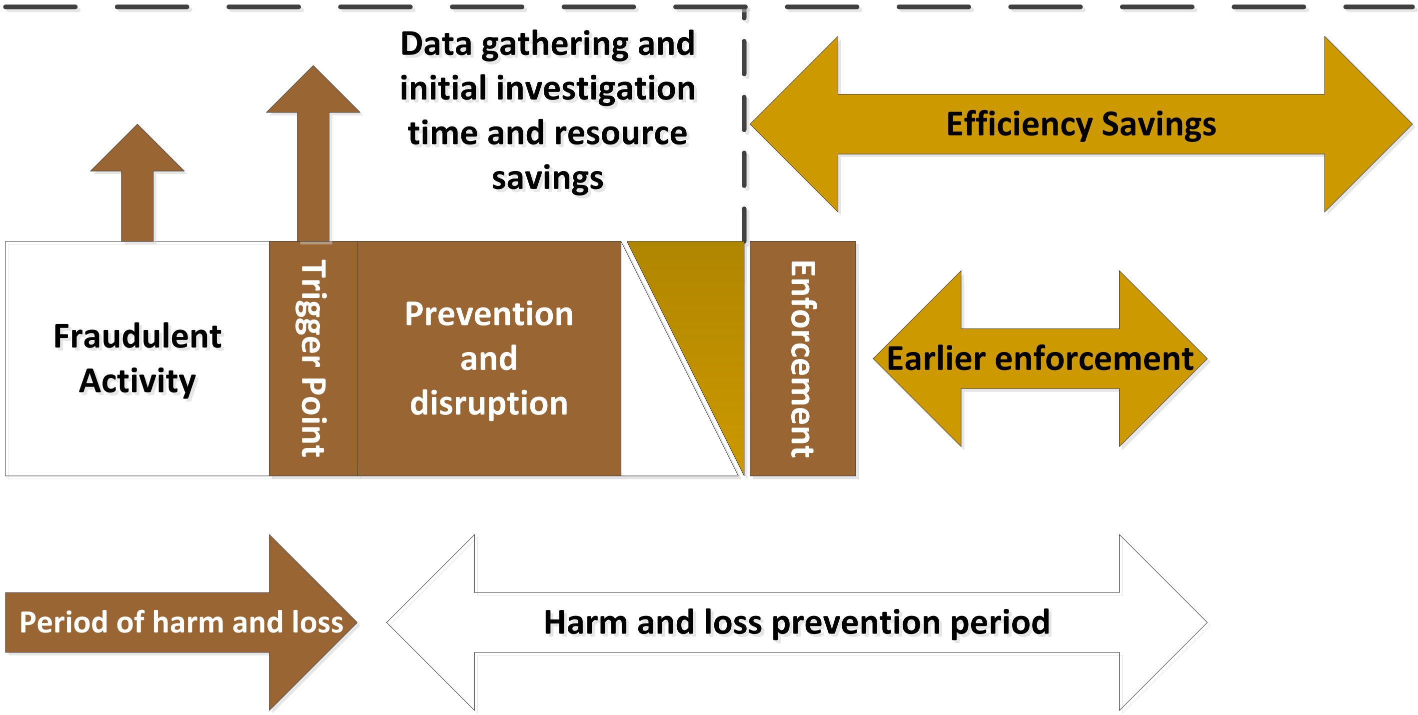
Next of kin details (Inform them that these persons may be contacted)	Name: DOB: For linking NOK to RMS Relationship:	
	Address: Telephone Mobile	
GP Details		

Does the victim consent to allow us to make referrals to Support Agencies on their behalf? **NOTE – In cases of safeguarding concerns, consent is overridden.**	Yes No

Please detail below any additional information the victim volunteered. Use your professional judgment to detail any areas of concern that you may have noticed during your contact (e.g. background noise, victim sounds nervous, are they still being contacted etc.)

Remember to complete an OEL entry detailing your contact with the victim. What action you may or not take within the VVA and to scan this document naming it **Direct assessment of needs** onto the occurrence under the victim's record.

APPENDIX 2 – FIM



APPENDIX 3 – Operation Signature Risk Assessment Template

Risk assessment for fraud, scam offences			
Victims name:			
History	How often do they receive mail, telephone calls, personal visits	5 4 3 1 0	Daily Weekly Fortnightly Occasionally Never
	How often do they send money	5 4 3 1 0	Daily Weekly Fortnightly Occasionally Never
	Have they been a previous victim of fraud	2 0	Yes No
	How much money have they sent	5 4 3 2 0	Over £10,000 £1000 - £10,000 £100 - £1000 Under £100 None
	When did the activity start. Is there a trigger for this activity	5 4 3 2 1	Over 10 years 5-10 years 2-5 years 1-2 years Under 1 year
Vulnerability	Do they live alone	2 0	Yes No
	Are they recently widowed/separated	2 0	Yes No
	Do they have a contactable next of kin. Are they local ?	3 2 0	No Yes – not local Yes – local
	Is there any evidence of scams taking place	3 0	Yes No
	Any other vulnerabilities evident Hoarder, victim of other fraud, door step crime etc	4 3 2 0	Affected a great deal Moderately affected Affected a little Not affected
	Is the suspect a family number	2 0	Yes No
	Do they have health issues Physical, mental health Visual/speech/hearing impairment Mobility	2 0	Yes No
	Do they have any other support Professional (SSD, carers) Friends	3 2 0	The victim is isolated from people who can offer support The victim has a few people to draw support on The victim has a close network of people
Maximum score of 46		**Total score**	
Standard 0-14	**Medium 15-21**		**High 22 and above**
These scores are there as a guide and should be used in conjunction of your own professional judgement of what advice, support and protection are required. Review the risk on the information you have.			
Person completing		**Date**	

APPENDIX 4 – Cease & Desist Letter

Our Ref: AF/ [Add Action Fraud Ref number]

Date: [Add date]

Dear [add name]

Re: Report Reference: [Niche crime number]

I write in connection with the above allegation of Fraud or Money Laundering [delete as appropriate] where your details have been provided.

North Wales Police have received a complaint of ………………… [Summarise what the person is accused of without revealing the victim details, for example "as the recipient of funds, which have been sent by victims of Fraud, for goods or services that have not been provided".

Activity of this nature could be interpreted as involvement in Fraud or Money Laundering, both of which are criminal offences.

If you have a reasonable explanation relating to this activity / your receipt of these funds, [Delete as appropriate] you may wish to email me to discuss the matter. In this case, please use the e mail address at the top of this letter.

Please be advised that if we receive further information of ongoing activity of a similar nature, it may result in a police investigation.

North Wales Police is committed to the reduction of Fraud and Money Laundering in our communities.

To achieve this aim, the force is working closely with agencies including the Crown Prosecution Service, Trading Standards, Action Fraud, National Fraud Intelligence Bureau and local authorities.

North Wales Police and its partner agencies will target any person, identified through intelligence, as being involved in Fraud or Money Laundering.

Intelligence has linked you to Fraud / Money Laundering [Delete as appropriate or if both apply, insert the word 'and' in place of the forward slash]. You will be part of the new approach.

There is a simple way to avoid this: have nothing to do with Fraud or Money Laundering.

Tactics that can be used against those identified include:

- ***A police officer can search any individual they have reasonable grounds to suspect has possession of any article for use in Fraud. (s. 1 of the Police and Criminal Evidence Act 1984).***
- ***A Warrant to enter and search premises may be obtained from the court.***
- ***You may be asked to account for your actions under Caution.***

- ***Your assets may be restrained or otherwise affected under Proceeds of Crime Act legislation.***

- ***Obtaining Anti-Social Behaviour Orders, to prevent individuals from frequenting certain areas or associating with other named individuals.***

- ***Eviction from homes if they are disrupting their neighbourhood.***

- ***Individuals involved in laundering criminal property may find that banking services are withdrawn and that their credit profile is affected.***

- ***These tactics and others will be used in a focused way against all those who are involved in Fraud and Money Laundering.***

Yours sincerely

APPENDIX 5 – 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.

HEDDLU GOGLEDD CYMRU

NORTH WALES POLICE

ECU FRAUD POLICY

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:**	2.0 – DRAFT
Effective Date:			
Recommended Review Date:			

CHANGE HISTORY				
Version No	**Date**	**Author**	**Changes**	**Ratification**
1.0		DCI	New policy	SLT
2.0	14/02/22	DC	Scheduled refresh	

CONTENTS

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.

- Adopts a proactive multiagency approach in preventing and reducing fraud.

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
- The **Direct Assessment of Need (DAN)** process (see Appendix 1) to ensure that vulnerable victims are correctly identified and supported
- An outline of the agreed National Fraud Reporting process whereby North Wales Police will direct any person wishing to report a fraud to the **Action Fraud** contact centre unless the case meets the agreed call for service criteria
- A requirement to follow the College of Policing Fraud Investigation Model (FIM) (See Appendix 2) 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)

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.

Most 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
- City of London Police Cyber Crime Key Assessment for North Wales Police
- City of London Police Fraud Profile for North Wales Police
- College of policing APP on investigating fraud
- Blackstones Investigation of fraud and economic crime
- HOCR and NCRS, Crime Recording Guidance Framework

4. ROLES AND RESPONSIBILITIES

4.1	**Force Control Room (FCC)**	• To follow the fraud CRE (see appendix 5) • To follow the fraud process map (see appendix 6)
4.2	**Any officer receiving a report of a fraud**	• To follow the fraud process map (see appendix 6)
4.3	**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 been incorrectly identified as having no vulnerability identified • To identify those most suitable for the fitting of call blockers • If required to conduct visits to vulnerable victims of fraud
4.4	**Cyber protect / pursue officer(s)**	• Assess and protect vulnerable victims of cyber enabled fraud as per the NFIB HO stats classes (Section 6.2) • To provide bespoke protect advice to attending officers of vulnerable victims of cyber enabled fraud to enable protect advice to be delivered • If required to conduct visits to vulnerable victims of cyber enabled fraud • To review requests from ECU fraud triage with regards to cyber related frauds and complete cyber related enquiries
4.5	**NWP Crime data integrity unit (CDIU)**	• To receive all fraud investigations from the NFIB and create occurrences. • 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.

4.6 Managed Response Unit (MRU)	• To follow the fraud process map (see appendix 6) • MRU supervisors to check the recording of ICAD occurrences from FCC • To identify those calls that have not met the CRE and to change the grading and advise the victim to follow the action fraud reporting route • To review occurrences to establish if they are slow time enquiries (P4) or if they need a response from the attendance of an officer/PCSO • To complete and EOEL 1 and EOEL 6 if a slow time investigation • To send master task to RMS ECU triage fraud pot
4.7 Economic Crime Unit (ECU) Fraud Triage	• To receive all fraud investigations from Action Fraud • To review and triage all fraud occurrences that come into the force via ICAD, officers or via third parties • Following triage to establish if the reported occurrences are to be investigated, for safeguarding, NFA or transfer to another force/NFIB using the CAT fraud triage matrix (see appendix 6) • To conduct desktop-based investigations of offences of fraud. • To allocate to the relevant department following triage. • Provide advice and assistance to Initial 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 Action Fraud in accordance with NCRS (National Crime Recording Statistics). • Record the NFRC number (the national crime number) in the ID NFRC number tab on NICHE. • To review all fraud cancellations, to add a rationale to the OEL and to request a cancellation with the NFIB • To request transfers via the transcrime process to NFIB crime registrars • To provide investigative advice with regards to election malpractice
4.8 FCIR (Force Crime and incident registrar)	• Review and ratify all outcomes ensuring that all incidents and crimes are recorded accurately and within directed timescales.
4.9 Managers/ Supervisors	• Ensure this policy is applied in your area of operations. • Ensure VCOP compliance is adhered to. • Where appropriate seek further ECU guidance when required • If a case is 12 months of age notify ECU D I and request a review.
4.10 ECU D I	• Have overall responsibility for updating the Fraud policy • Complete dip sampling of all active fraud investigations • Ensure that staff within the ECU and all other staff with fraud responsibility receive appropriate training.

5. THE FRAUD REPORTING PROCESS

5.1 Reporting Fraud Offence – REPORT FRAUD

Action 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.

A vulnerability assessment should be undertaken by the Force Control Room. If the victim is reporting a fraud this will launch the CRE process that will allow the FCC to conduct an assessment and if following the CRE it is found that it is not met then the FCC should be advising the victim to report the matter to Action Fraud and creating the call as a contact record.

5.2 Vulnerability Assessment

Role	Action Required
5.2.1 **Force Control Room/ Any Officer receiving a report of a fraud**	• Create on ICAD a report of fraud to launch the CRE process and undertake a **Vulnerability Assessment** where a victim is reporting fraud ***prior*** to advising them to report the matter to **Action Fraud**. • follow the **CRE Process for fraud** • follow the fraud process map for allocation to ECU fraud triage. • See sections 5.3 & 5.4 below
5.2.2 **Initial Investigating Officer & Supervisors**	*Please note*: 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 Action Fraud. **If the person reporting is vulnerable or the case meets the 'call for service' criteria you should then:** • 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, financial investigation. Fraud SPOC's within District CID, or Financial Abuse Safeguarding Officer (FASO). • Do **NOT** submit the crime for filing *until* an NFRC is obtained and placed on the OEL. This will be obtained by the ECU fraud triage team. If the victim is unable to report the matter to Action fraud the initial responder should assist or complete the report on behalf of the victim.

5.3 Offences not recorded by Action Fraud

Do **NOT** report the following fraud offences to Action Fraud

- If a report of fraud requires either immediate police action **or** involves a vulnerable victim
- making, supplying or use of articles to commit fraud*
- possessing/controlling article(s) for use in fraud*
- possession of false documents*

- theft of fuel*
- forgery or use of drug prescription*
- fraud or forgery relating to vehicle or driver records*
- other forgery*
- Blackmail* (however there may be a cyber element)
  (***** these are ***not*** recorded by Action Fraud)

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

All other reports of fraud (including Live Cyberattacks) should be made to **Action Fraud** via their website www.actionfraud.police.uk or by telephoning **0300 123 2040**. (For more details, see Flow Diagram on page 8)

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

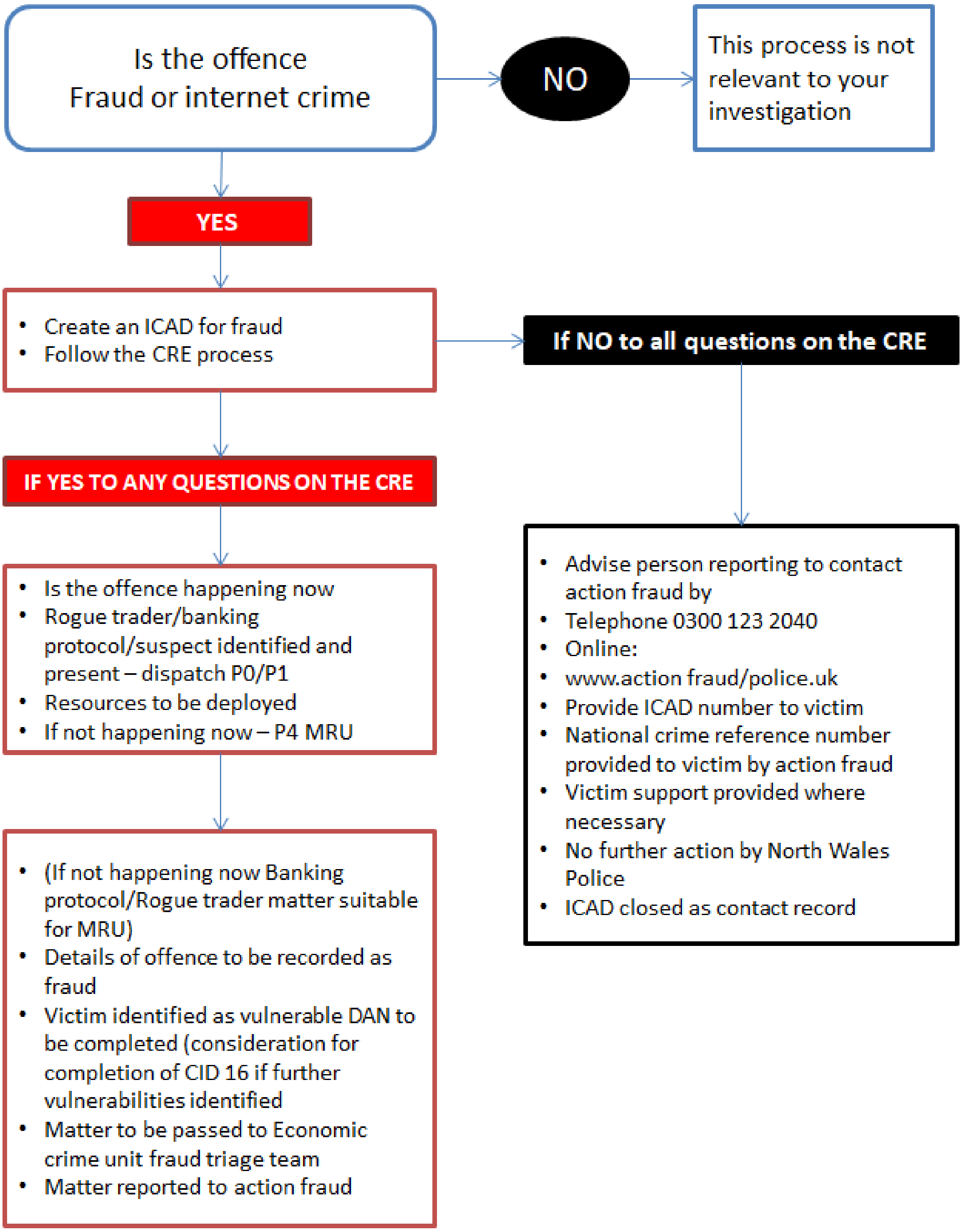
- Create an ICAD log/occurrence
- Circulate the vehicle/equipment on PNC.
  (PNC 'Registered item' Action Fraud does not have access to the Police National Computer (PNC) and therefore will be unable to record crimes where a PNC 'registered item' (vehicle, plant, machinery etc) requires an entry on PNC. Police will be responsible for reporting these offences to the NFIB, 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 from the NFIB rather than Action Fraud to a vault to which CDIU supervisors and the ECU fraud SPOC have access.
CDIU also record all 'call for service' frauds on Niche and apply a classification in line with HOCR NFIB codes. Thereafter they will be tasked to the NICHE RMS allocations pot for ECU fraud triage (NWP_ECUfraudtriage), desktop investigation and allocation (if required).

All Transfer of Crime / Cancellation requests in relation to NFIB (Action Fraud) recorded fraud must be submitted to the ECU fraud triage SPOC who will submit to the NFIB FCIR.

5.6 North Wales Police initial Fraud Reporting Process Flowchart



6. VULNERABILITY ASSESSMENT FOR VICTIMS OF FRAUD/CYBER

In accordance 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.

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 initiative 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 referred to suitable partner agencies;
- 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**	• Initially review the Action Fraud data • Prioritise it into the following six categories:

	1. Aged 70+ 2. Aged 60-69 years 3. Other victims who identify to Action Fraud that they have been significantly affected by what happened (Aged 0 – 59) 4. Aged 0-59 5. Organisation 6. No Date of birth listed • Also review The Action Fraud data to identify repeat victims (including repeat businesses).

6.3 All Victims Aged 70 and Over

Role	Action Required
6.3.1 **Force Control Room / Any Officer received a report of fraud**	• The Force Control Room Staff will follow the Customer Rules Engine 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 the ICR document on the Pronto system. • Complete a CID 16 referral to notify other agencies. • Provide Crime Prevention advice as appropriate to the circumstances.
6.3.3 **FASO**	• Review the Direct Assessment of Needs using **Operation Signature Risk Assessment Template** (see Appendix 3). • Place on the OEL an outline of any additional safeguarding or support that is required from the Safer Neighbourhood Team. This occurrence is then re-tasked back to the PCSO or Police Officer who completed the initial DAN or to the relevant crime allocations pot for the area concerned for allocation if required. • Actively monitor tasks that have been sent to the respective allocations pots within NICHE for safeguarding visits. • Once they are completed, to risk assess the victim using the Operation Signature Risk Assessment Scoring Model to identify any further needs. • Complete referrals to Victim Help Centre • Consider disruption action to protect victim(s)

6.4 Victims Aged Under 70

These victims may also receive a personal visit if they are:

- a repeat victim
- or from the information provided they are identified as vulnerable

Role	Action Required
6.4.1 **FASO**	• Provide crime prevention advice by email (if email address is available) along with your contact details so that victims can make contact with the FASO if they require any additional advice or support.

	• Examine data within the Action Fraud data to establish websites, email addresses and telephone numbers of the suspects for purposes of disruption. • If the victim has been using Money Service Bureau's (MSB's) to transfer money to suspects the FASO will consider making contact with SPOC's within those MSB's to have their accounts temporarily suspended to prevent further offences. • Monitor all events of 'Banking Protocol' to ensure that the Banking Protocol is being complied with. • Share the information with the relevant trading standards departments if applicable. • In the event of any breaches of Banking Protocol contact the coordinator at UK Finance. • Share the Banking Protocol returns with the Cyber Protection Officer at the City of London Police on a ***monthly*** basis.

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 a 'crime in action' call for service, must be a recorded crime and a criminal investigation and referral in to 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

The fraud triage matrix is based upon the crime allocation triage (CAT) system that was introduced for the scoring and allocation of investigations that have upon them a CID 16 or that are recorded under a particular crime type. This matrix is used by Detective Sergeants within CID, any occurrence that scores over 55 are allocated to CID for progression.

It was decided that any matrix should follow an already agreed process using an already recognised document; this will bring uniformity and trust to the document.

The matrix has been re-written so that it covers vulnerability, types of fraud, threat, harm, risk to the victim/business and any opportunities that are available to disrupt the suspect(s).

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 fraud SPOC, dedicated investigation team or fraud investigator based within the ECU.

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

Not to progress with an investigation – initial considerations

- The investigation would require a disproportionate level of resources to bring the case to a conclusion and would adversely impact upon our ability to investigate other crimes.

- The victims 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. (eg 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 victim has pursued civil recourse and has subsequently turned to the police for a criminal investigation as a result of dissatisfaction with the civil remedy.
- Delays to the investigation will be caused by the location of key evidence elsewhere.
- Victims have ignored guidelines that are designed to prevent them becoming victims of fraud, for example, online banking and auction sites.
- Frauds where the victim's conduct has contributed to the loss, in particular, where the police have previously given guidance or warnings to victims about fraud risks that have not been acted upon.
- Cases where the victim's motive for making the complaint appears to be malicious and is primarily focused on recovering monies owed, or designed to distract attention from the complainant's own involvement in the fraud. (Such cases might nevertheless merit investigation, particularly where there are other victims involved).
- Cases where victims are not prepared to co-operate fully with the investigation and prosecution, although we will always consider carefully how to assist victims and witnesses who have concerns about safety.
- Frauds more suitable for investigation by another enforcement or regulatory agency.
- Cases where another police force has decided not to investigate other than for geographical reasons.
- Frauds that have already been investigated by the police or another enforcement agency, or that have been the subject of regulatory proceedings, unless significant new evidence has come to light or the previous investigation had a narrow remit that did not address all the relevant issues.
- Cases where the existence of other proceedings might have a detrimental effect on a criminal investigation and subsequent prosecution.
- Frauds which took place a long time ago (probably more than 2 years), unless there are exceptional circumstances.

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:

- **Patrol Officer/PCSO**
- **CID Officer**
- **Cyber Crime Team Officer**
- **Economic crime unit fraud investigator**
- **To set up a dedicated investigation team**
- **or to consider <u>no investigation</u> or <u>alternative resolutions</u>**

9. NO INVESTIGATION

If the decision is to ***not*** investigate: -

- 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.
- **Outcome type 21** is to be used to file the case on RMS and NFIB 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 <u>not</u> 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 <u>*must*</u> be informed of the decision in writing/email.

Role		Action Required
9.1	**Force Crime and incident Registrar**	• Periodically review the application of outcome 21 to ensure the highest standards of integrity and victim focus. • Refer unsuitable cases to the respective Divisional Crime Manager for further consideration for a full investigation.

Standards of Outcome 21 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. All such cases must be referred to the Divisional Crime Manager for authorisation <u>***before***</u> the victim is informed of the outcome.

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 dedicated fraud SPOC within the ECU fraud triage team will review all requests for cancellations of fraud occurrences. They will add an entry onto the OEL and if the matter has already been reported to the NFIB the SPOC will request a cancellation of that crime which is held by the NFIB. 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 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.	• **Criminality notice to offender** • **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** • **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.**
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 (noting the offenders are mainly abroad).**
Mandate Fraud	• **Criminality notice to offender**

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.	• **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.**
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.**
Intellectual Property Fraud This is when fake goods are passed off as originals and effects many industries including health, music, film, fashion and fragrances.	• **Refer to Trading Standards** • **Refer to the Intellectual Property Office** • **Refer to FACT (Federation Against Copyright Theft) if music or film related offences**
Domain Name Scams This scam is offering businesses first refusal on a domain name, suggesting someone else is just about to buy it or by sending out bogus domain name renewal notices.	• **Criminality notice to offender** • **Submit intelligence accordingly on niche** • **Advise victims by letter of outcome and offer crime prevention advice** • **Refer to Nominet to consider whether abusive registration**

10.2 Mass Marketing and Miscellaneous Fraud

Type of Fraud	Potential Alternatives to investigation may include the following:
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	• **Criminality notice to offender** • **Refer to Trading Standards to use bespoke powers if they wish to proceed** • **Submit intelligence accordingly on niche**

materialise using the internet or telephony.	• **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.**

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 *<u>money laundering offence</u>*.** • **Submit intelligence accordingly via niche with correct dissemination (noting the offenders are mainly abroad).**
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.	• **Criminality notice to offender** • **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.**
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** • **Criminality notice to offender** • **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 visit 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**
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)** • **Criminality notice to offender** • **Submit intelligence accordingly on RMS** • **Advise victim of the outcome**
Mail Scams Legitimate mail boxes and post redirections can be used in the application of fraud.	• **Criminality notice to offender** • **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.	• **Criminality notice to offender** • **Intelligence to be submitted accordingly on niche** • **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.
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 visit to business premises with Trading Standards and DWP and criminality notices served** • **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

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.	• **Criminality notice to offender** • **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**
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. (NFRC number per account not per victim)	• **Criminality notice to offender** • **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.**
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	If these organisations will not undertake an investigation, • **Disruption visit to business premises with appropriate above agencies and criminality notices served**

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.	• **Intelligence to be submitted accordingly on RMS** • **Victims to be advised of the outcome and crime prevention advice offered**

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. As such FIU should be notified so a POCA asset review can be undertaken and an investigation strategy formulated.

Role	Action Required
10.5 Fraud triage officer	• Justify this decision • Provide guidance and advice to investigators in relation to points to prove alongside the relevant investigation strategy.

11. FRAUD INVESTIGATION PROCESS

NFIB 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 NFIB and if not this will be challenged by the CDIU supervisor or by the by the Fraud SPOC who is sat within the ECU fraud triage team at the earliest opportunity or through the Force Crime & Incident Registrar

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 by the divisional Single Point of Contact.

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

- Patrol Officer/PCSO
- CID Officer
- POVA/PVPU
- Economic crime unit cyber crime team protect/pursue officer
- Economic crime unit fraud investigators
- to set up a dedicated investigation team
- 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.

A decision will then be made by the ECU upon allocation of these occurrences to either PVPU or to be retained within the ECU for progression. PVPU will be asked to review any threat, harm and risk that can be addressed via mainstream safeguarding procedures.

Due to the structures of the national Action Fraud and NFIB, all Cyber Dependent offences received by Action Fraud are processed by NFIB 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 decided following consultation with the Divisional Crime Manager, Cyber Crime Manager and ECU Manager.

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 Cyber Crime Unit, ECU, Patrol Officers and divisional CID Teams is key to ensuring open discussions in the interest of the victim 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 an 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.

12. MONEY MULE PROCESS

12.1 Role of a Money Mule

A money mule (sometimes called a "smurfer") is a person who transfers money acquired illegally (e.g., stolen, obtained through fraud) in person, through a courier service, or electronically, on behalf of others. The money is transferred from the mule's account to the scam operator, typically in another country.

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. Some money mules are recruited via dating sites/romance scams.

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 true identity and location from the victim of the crime and the authorities. By using instant payment mechanisms such as Western Union, 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 Action Fraud that indicates the recipient account of fraudulent funds.

Depending on the circumstances and nature of the report/intelligence, there may be a clear suggestion that the person involved is in fact highly vulnerable and as much a victim themselves as well as being complicit in the transfer of potential criminal monies (e.g., as part of a dating/romance fraud).

12.2 The 3 stage process for the escalation of police intervention in such circumstances

Stage 1 **At this triage stage, it is likely the incident will have been allocated for a safeguarding visit.**	**The Officer/PCSO** • Serve a warning letter on them outlining that they are potentially laundering the proceeds of crime and must stop. • Complete a proforma statement detailing that this warning has been given. • Update the Op Signature safeguarding “non-counting” Niche Occurrence. Safeguarding should still be considered for the victim and any other person identified sending monies. This is also to be recorded on the incident. If the (Muling) activity continues: If the victim continues to receive and send monies after initial police intervention, the offence of money laundering under S327 Proceeds of Crime Act (convert/transfer criminal property) is potentially made out. The rationale being that the subject should have “known or suspected” the proceeds are derived from crime because an attending officer has previously advised them so.
Stage 2 **The occurrence will be assessed and allocated as per force policy to an officer to investigate.**	• A separate Niche Crime Occurrence will be created for the offence of Money Laundering. The victim will now be recorded as a suspect of that offence and following initial enquiries (where possible) invited for Voluntary Attendance/interviewed under caution bearing in mind any identified vulnerabilities. Once an account has been gained from the suspect a decision can be made as to the scope of any investigation and likely outcome. Given the nature of the vulnerabilities identified by the **Op Signature process** (see Appendix 3), on the first occasion a suspect is interviewed/investigated it is highly possible that a decision will be made that the matter is not suitable for prosecution/NFA (consider HO Outcome 10, 15, 16 or 21). However, the process of conducting a formal, recorded interview under caution allows police to capture the suspect “knowledge or suspicion” in an evidential format. Suspects should be advised as part of the interview process that the record of interview may be used in future proceedings should the

	activity continue. Consideration should also be given to the service of a Cease & Desist letter at this time.

Stage 3 **In those cases where, after previous intervention a suspect persistently continues to engage in muling activity**	• A separate Niche Crime Occurrence (Money Laundering) will be created again. If necessary or appropriate the suspect will be arrested or invited for Voluntary Attendance/interviewed under caution, and a file submitted to CPS if appropriate. Following advice from the CPS, it is recommended that consideration be given to exploring the use of CBO`s post-conviction, or SCPO`s (which are available on a standalone civil basis) as an alternative method of disposal, or means of controlling muling behaviour.

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 college of policing code of ethics (2014).

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 – DIRECT ASSESSMENT OF NEED (DAN) FORM

Name		Date of birth	
Address			
Telephone		Mobile	
Email address			

Attendance date		Attending officer		RM/RC	

Did the victim initially report the fraud to the police ?	Yes/No
Was the victim advised to contact Action fraud ?	Yes/No

How has the victim been contacted	Phone	
	Email	
	Post/Mail (Consider seizing mail)	
	In person (door step)	
	Other	

How frequent has contact been made ?									
Daily		Weekly		Fortnightly		Occasionally		Never	

Has the victim sent any money ?				Yes/No			
Under £100		£100 - £1000		£1000 – £10,000		Over £10,000	

How frequent has money been sent ?									
Daily		Weekly		Fortnightly		Occasionally		Never	

How has the victim sent money – tick as many as appropriate											
Cheque		Cash		Bank card		Money transfer		Postal order		Other	

Provide details of suspect: Names provided, account numbers, sent cheque numbers, postal orders, recipient addresses, e mail addresses, reference numbers of MSB (money service businesses)

When did the activity start?									
Under a year		1-2 Years		2-5 years		5-10 years		Over 10 years	

What (if anything) triggered this activity? (e.g. death of a spouse)
Provide details of the victim's bank account (if they have been transferring from that account).

How affected are they by what has happened to them?							
Affected a great deal		Moderately affected		Affected a little		Not affected	

Do they have a support network? Family, friends, neighbours? What social interaction do they have?	Yes/No - Specify
What type of fraud/scam has/is taking place	

Dating/romance Health, medical		Lottery/Prize draws		Investment Inheritance		Computer software	
Door to door, rogue trader		Catalogue		Clairvoyant's		Courier/Telephone	

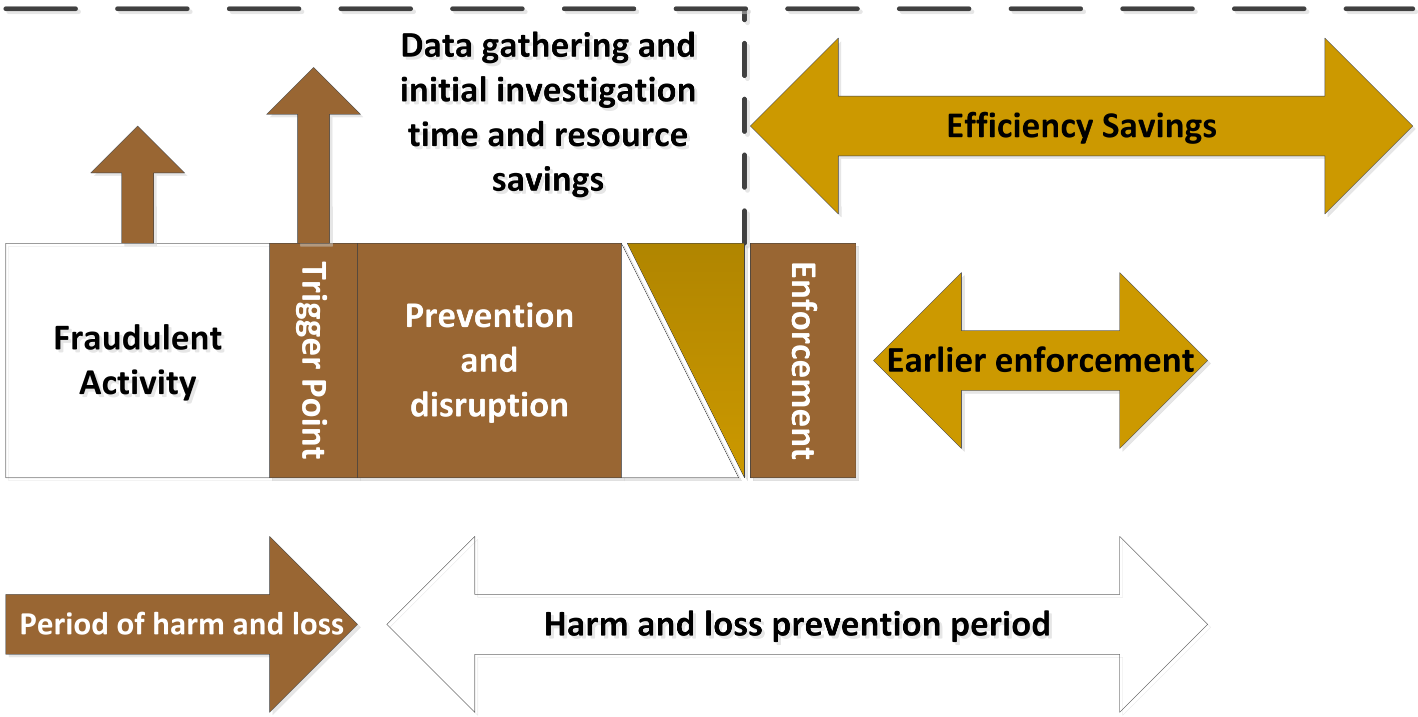
Are there any other vulnerabilities evident: Does the victim feel threatened, intimidated, frightened, and isolated? Pregnant, hoarder, victim of any other fraud type offences, cold callers, rouge traders other doorstep crime. Do they have any children/dependants?	Yes/No

Do they have any health issues? Consider: Physical, Mental health Visual/speech/hearing impairment mobility	Yes/No - Specify		
Do they live alone?	Yes/No	Are they recently widowed/separated	Yes/No
Does the victim have any home care support	Yes/No	Company name & telephone number	
Next of kin details (Inform them that these persons may be contacted)	Name: DOB: For linking NOK to RMS Relationship:		
	Address: Telephone Mobile		
GP Details			

Does the victim consent to allow us to make referrals to Support Agencies on their behalf? **NOTE – In cases of safeguarding concerns, consent is overridden.**	Yes No

Please detail below any additional information the victim volunteered. Use your professional judgment to detail any areas of concern that you may have noticed during your contact (e.g. background noise, victim sounds nervous, are they still being contacted etc.)

15. APPENDIX 2 – FIM



16. APPENDIX 3 – OPERATION SIGNATURE RISK ASSESSMENT TEMPLATE

Risk assessment for fraud, scam offences				
Victims name:				
History	How often do they receive mail, telephone calls, personal visits		5 4 3 1 0	Daily Weekly Fortnightly Occasionally Never
	How often do they send money		5 4 3 1 0	Daily Weekly Fortnightly Occasionally Never
	Have they been a previous victim of fraud		2 0	Yes No
	How much money have they sent		5 4 3 2 0	Over £10,000 £1000 - £10,000 £100 - £1000 Under £100 None
	When did the activity start. Is there a trigger for this activity		5 4 3 2 1	Over 10 years 5-10 years 2-5 years 1-2 years Under 1 year
Vulnerability	Do they live alone		2 0	Yes No
	Are they recently widowed/separated		2 0	Yes No
	Do they have a contactable next of kin. Are they local ?		3 2 0	No Yes – not local Yes – local
	Is there any evidence of scams taking place		3 0	Yes No
	Any other vulnerabilities evident Hoarder, victim of other fraud, door step crime etc		4 3 2 0	Affected a great deal Moderately affected Affected a little Not affected
	Is the suspect a family number		2 0	Yes No
	Do they have health issues Physical, mental health Visual/speech/hearing impairment Mobility		2 0	Yes No
	Do they have any other support Professional (SSD, carers) Friends		3 2 0	The victim is isolated from people who can offer support The victim has a few people to draw support on The victim has a close network of people

score of 46	Maximum	Total score		
Standard 0-14	Medium 15-21			High 22 and above
These scores are there as a guide and should be used in conjunction of your own professional judgement of what advice, support and protection are required. Review the risk on the information you have.				
Person completing		Date		

17. APPENDIX 4 – CEASE & DESIST LETTER

Our Ref: AF/ [Add Action Fraud Ref number]

Date: [Add date]

Dear [add name]

Re: Report Reference: [Niche crime number]

I write in connection with the above allegation of Fraud or Money Laundering [delete as appropriate] where your details have been provided.

North Wales Police have received a complaint of ………………… [Summarise what the person is accused of without revealing the victim details, for example "as the recipient of funds, which have been sent by victims of Fraud, for goods or services that have not been provided".

Activity of this nature could be interpreted as involvement in Fraud or Money Laundering, both of which are criminal offences.

If you have a reasonable explanation relating to this activity / your receipt of these funds, [Delete as appropriate] you may wish to email me to discuss the matter. In this case, please use the e mail address at the top of this letter.

Please be advised that if we receive further information of ongoing activity of a similar nature, it may result in a police investigation.

North Wales Police is committed to the reduction of Fraud and Money Laundering in our communities.

To achieve this aim, the force is working closely with agencies including the Crown Prosecution Service, Trading Standards, Action Fraud, National Fraud Intelligence Bureau and local authorities.

North Wales Police and its partner agencies will target any person, identified through intelligence, as being involved in Fraud or Money Laundering.

Intelligence has linked you to Fraud / Money Laundering [Delete as appropriate or if both apply, insert the word 'and' in place of the forward slash]. You will be part of the new approach.

There is a simple way to avoid this: have nothing to do with Fraud or Money Laundering.

Tactics that can be used against those identified include:

- ***A police officer can search any individual they have reasonable grounds to suspect has possession of any article for use in Fraud. (s. 1 of the Police and Criminal Evidence Act 1984).***

- ***A Warrant to enter and search premises may be obtained from the court.***

- ***You may be asked to account for your actions under Caution.***

- ***Your assets may be restrained or otherwise affected under Proceeds of Crime Act legislation.***

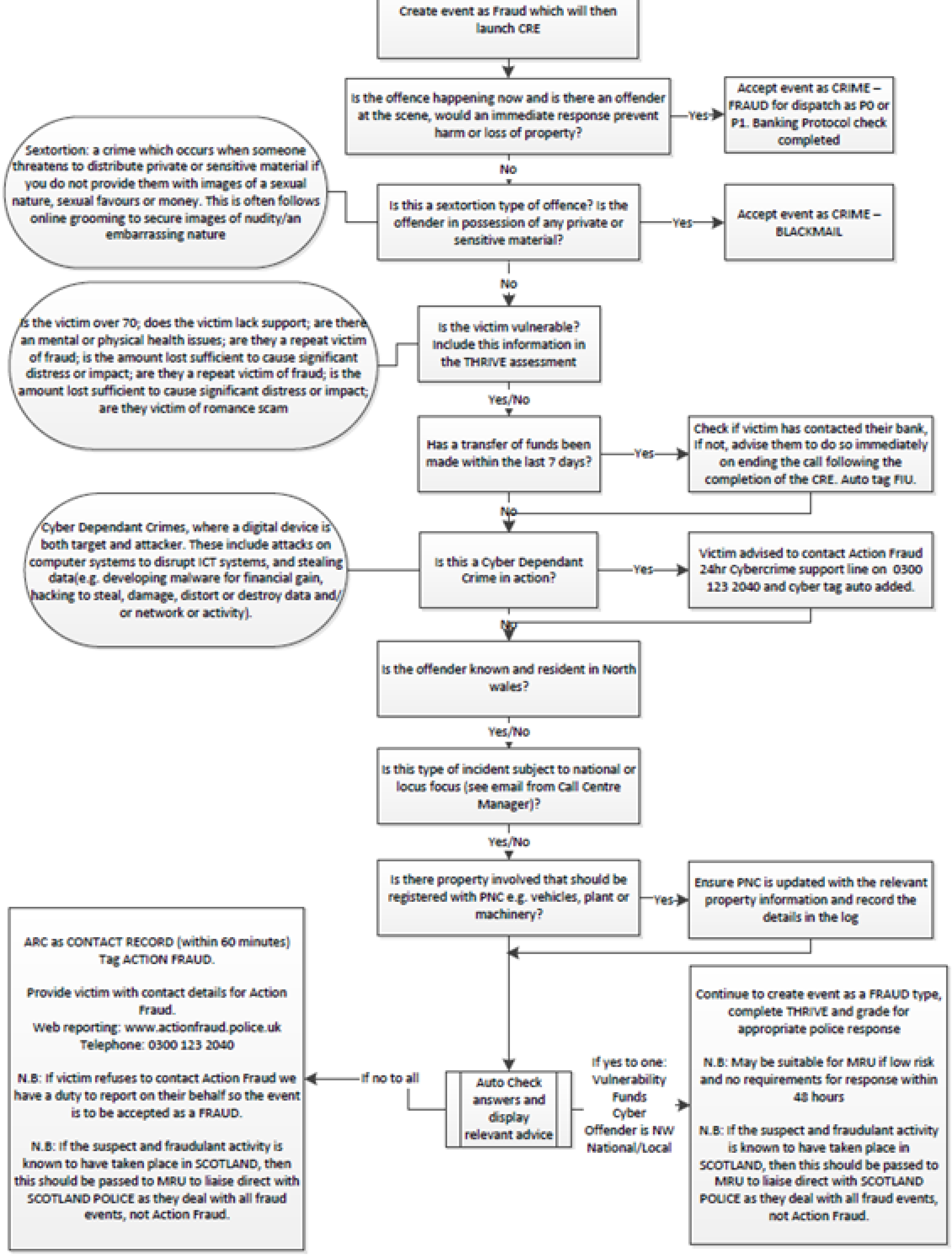
- ***Obtaining Anti-Social Behaviour Orders, to prevent individuals from frequenting certain areas or associating with other named individuals.***

- ***Eviction from homes if they are disrupting their neighbourhood.***

- ***Individuals involved in laundering criminal property may find that banking services are withdrawn and that their credit profile is affected.***

- ***These tactics and others will be used in a focused way against all those who are involved in Fraud and Money Laundering.***

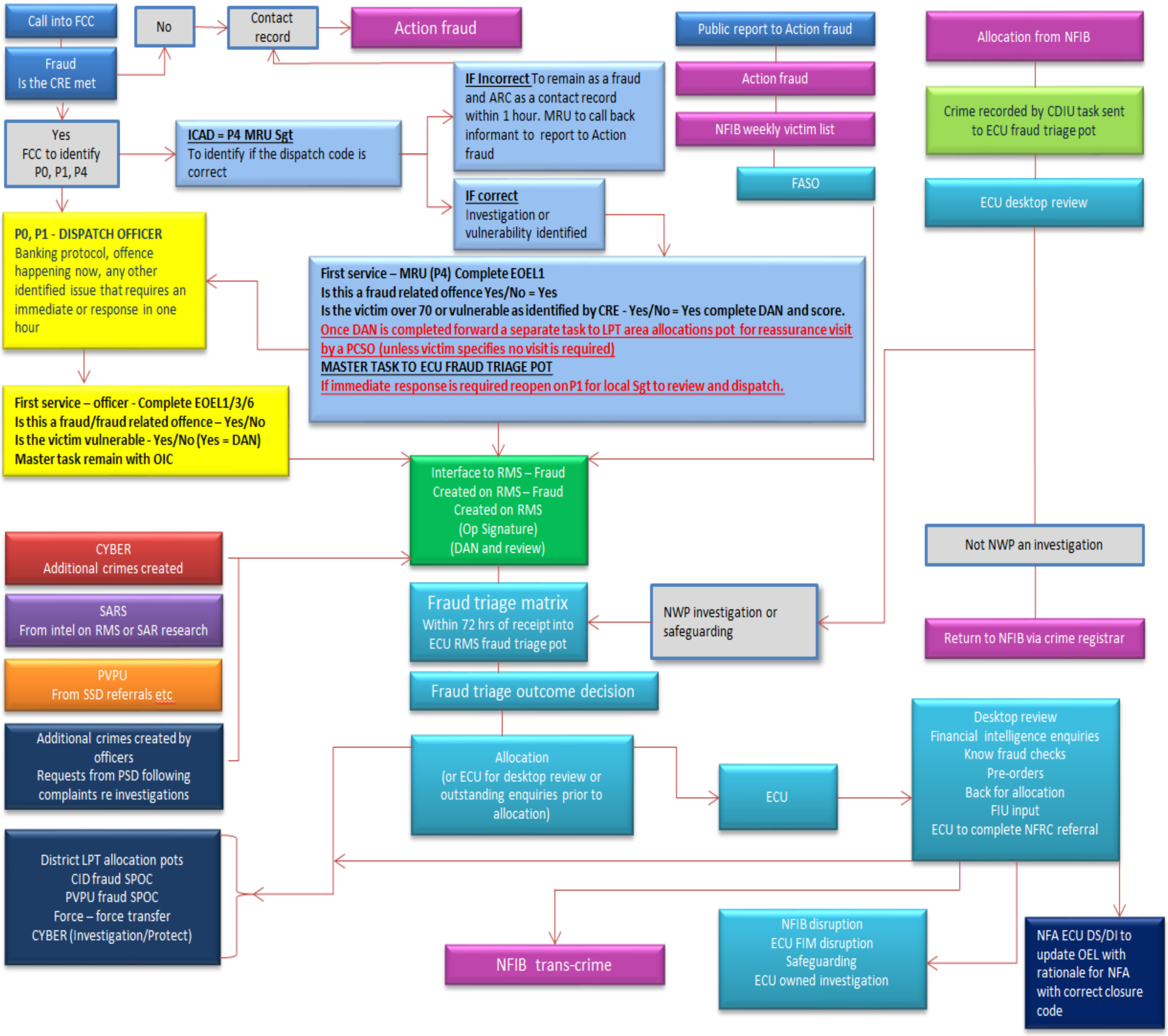
Yours sincerely



18. kAPPENDIX 5 – FCC FRAUD CRE

19. APPENDIX 6 – ECU FRAUD PROCESS MAP

u



20. APPENDIX 7 – ECU FRAUD TRIAGE

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.**
Opportunitie s	**Please select.**
Total score	
Allocation	**Please select.**
Area	**Please select.**
CAT REFERENCE	**#CATSCORE00**
Comments	

21. APPENDIX 8 – 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.