

National Policing Strategy for the Victims of Fraud

Draft prepared by the National Police Coordinator for Economic Crime April 2015

SUPPORTING THE VICTIMS OF FRAUD

Introduction: This is the National Policing Strategy for the victims of fraud, produced by the National Police Coordinator for Economic Crime (NPCEC). We are developing this through the Crime Business Area in consultation with chief police officers and their staff. It is part of the national policing strategy for fraud and is designed to assist chief officers in delivering the most appropriate support to victims of fraud in their community. This document is best read in the context of the National Policing Fraud Strategy which set out the aim of reducing the impact of fraud (its volume, value and impact on people). Where policing failed to protect the community from fraud it set the objective of "supporting victims of fraud ensuring that they receive an appropriate service from policing in partnership with other agencies such as Victim Support and other Government departments (such as Social Services)".

Strategy Aim: The **aim** of this strategy is to put in place a system that delivers the appropriate care to victims in a consistent and responsive manner. We will ensure that victims of fraud, individual or corporate, receive the support they need, at the time they need it, for as long as they need it with particular emphasis on addressing the needs of the vulnerable and repeat victims. It will do this **by** putting in place the mechanisms to:

- Identify victims at the point of reporting (normally to Action Fraud) and provide initial assessment of individual need.
- Notify them to the appropriate police force.
- Provide an escalated response to meet individual levels of need.
- Engage with agencies available to assist policing in supporting victims.

We will use the above structure to deliver:

- An initial response to victims.
- Ongoing support to victims dependent on need.
- Protection from further victimisation.

A successful outcome will have been achieved when:

- The national processes are in place and operating
- Force areas have put in place effective victim care plans

> Victims and their champions nationally, report that their victim needs are being met.

THE NEED

The need for a strategy for the victims of fraud in addition to that adopted for victims of other crime types is two-fold:

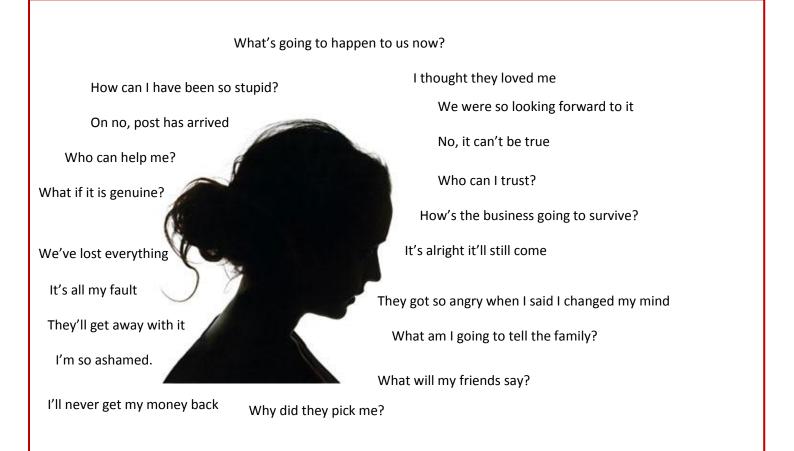
- Nature of fraud victimisation.
- Nature of the operational response to fraud.

Fraud Victims: A short discussion on the nature of fraud victims is attached at Appendix 1. In essence far from being the victimless crime it is sometimes claimed to be Fraud often has a disproportionately high monetary and emotional impact on victims. To compound matters, fraud victims are often repeatedly targeted to the extent even of victim details being sold from fraudster to fraudster.

Value A physical acquisitive crime (though fraud can have a physical element to it) will, in general, be limited to those assets, cash or property, immediately available and transportable at the time and location of the crime. In the case of fraud the victim can be inveigled over time to give over their entire savings and indeed more, regardless of the form in which the assets were held by the victim.

- Emotional Impact There are a number of aspects of fraud which can serve to make the emotional impact of fraud particularly acute.
 - Guilt Virtually by definition most victims of fraud will have unwittingly cooperated in the offence by transferring assets to the criminal or compromising their identity. This can lead to feelings of guilt. embarrassment and loss of self-confidence. Additionally, victims may perceive others as viewing them as having brought the crime upon themselves through stupidity or greed.
 - > Disappointment Victims will often have entered the relationship with the criminal in order to meet an emotional need or desire. be it а financially secure future, the meeting of religious or social obligations, a desired product, meaningful relationship, 'fun'. commercial revenue etc. Not only is this need not fulfilled but the opportunity to meet the need may be past or now unaffordable.

Trust Again virtually by definition, the victim will have placed trust in the fraudster to provide something in return for the money they are committing. At its simplest this will be the trust of a customer / supplier relationship but can be more emotionally complex when, for example, the fraudster plays on trust based on professional standing, authority or a personal relationship. It may take victims a period of time to accept that their trust was misplaced and this breach of trust will have an emotional impact.



Operational Response to Fraud

Fraud, particularly when enabled by cyber technology, is not bound by geography. As a result the police response to this has been one in which fraud is reported centrally, collated, analysed and then disseminated to the most appropriate local force for investigation. This means that unlike other crime types there is likely to be a dislocation between the investigating force and the victim. Furthermore, the victim of physical crime types receives a visible police presence including perhaps a uniformed first response, needed); reassurance and an outline of the likely process that will be followed. The victim of fraud is currently unlikely to receive the same support.

OUR STRATEGIC RESPONSE

Vision Policing will work with partners to put in place an effective, affordable and reliable system to ensure victims of fraud, individual or corporate, receive the support they need, at the time they need it, for as long as they need it. The system will ensure that victims of fraud receive a service which, as a minimum, is comparable to the best of that provided to victims of other acquisitive crime. As a result of the support, victims will be able to avoid ongoing or repeat victimisation. Support to victims of fraud will have an reputation enhanced encouraging other victims to report crime and raising confidence in the police service. There will be a close correlation between support to victims and crime prevention (Protect). Crime intelligence and victimology study by the National Fraud Intelligence Bureau (NFIB) will be used to help inform strategic and tactical inform decisions

crime scene examiner and detective; they receive the details of a point of contact, prevention advice (or action if about the scale and nature of support to victims and predict demand.

Design Principles The victim support system will be constructed with a number of principles in mind:

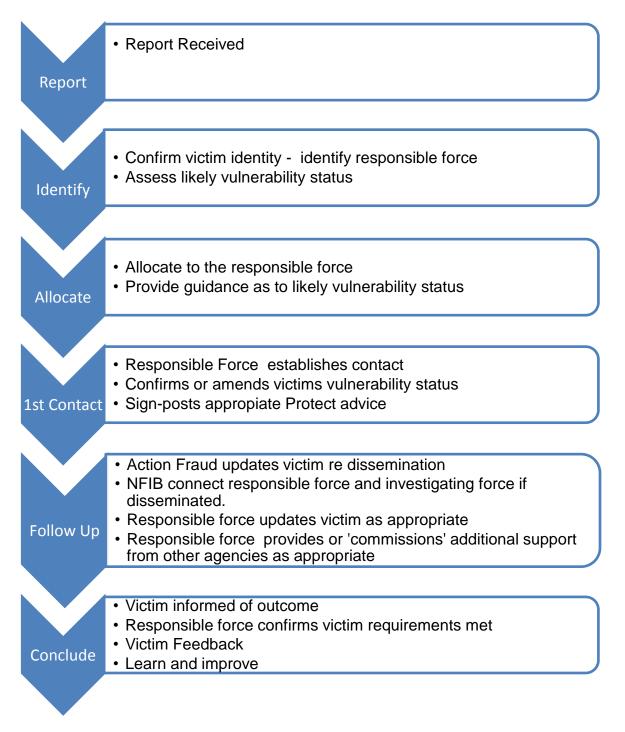
- Support should commence as close to the time of the victim reporting the crime as practicable.
- The first priority is to prevent further harm to the victim.
- Response is graduated and tailored to the needs of the victim with particular care given to those who might be vulnerable or likely to become repeat victims.
- The system will meet and where possible exceed all applicable directives and codes of practice.
- The support system will be accessible to all, consistent, make best use of existing resources, be transparent and quality assured.

The System

The system will normally be initiated at the point at which a crime is reported to Action Fraud. The report will be analysed to establish the victim identity, the force in whose area the victim is normally resident (referred to

in this document as "the responsible force") and a guide as to the vulnerability status of the victim. The responsible force will provide support to the victim according to need either directly or through outsourcing to other agencies or organisations. Where a case is disseminated NFIB will inform the responsible force of the identity of the investigating force and the crime number. The responsible force will seek updates from the investigating force on behalf of the victim (the proposed joint fraud crime management system will facilitate this).

THE END TO END SYSTEM



 Report & Identify Victims will continue to report to Action Fraud through the call centre, internet or, exceptionally, though their local force. Action Fraud will ensure they record sufficient detail to identify the responsible force and to enable an assessment to be made and guidance offered as to the level of vulnerability of the victim.

- Allocate NFIB will allocate victims responsible force to the and provide guidance as to their likely vulnerability. This guidance will be based on individual factors as recorded by Action Fraud with added value from local victimology intelligence (NFIB currently inform all forces of victims in their area through Polka but the intention will be to provide a more direct service to forces following IT modernisation).
- 1st Contact As soon as practicable after receiving an NFIB Victim referral the responsible force will make contact with the victim in their area. The nature of the first contact will be a matter of local policy and according to need / vulnerability. At its simplest this may be undertaken by phone call to the victim though personal visit will in many cases be more appropriate. Forces will use a variety of resources for this including PCSOs, Special Constables or other forms of volunteer staff. The National Economic Crime Academy is able

to provide training to equip force staff for this. Contact with the victim will differ from that for other crime types in that the aim is not that of protecting a physical crime scene or securing evidence. Instead the priorities for this contact are to:

- Protect the victim from further harm eg establish that the victim is not still involved in transactions or communications with the criminals (a not unlikely situation (see 'Fraud Victim's above)).
- Confirm or amend the assessment of vulnerability provided by NFIB.
- Provide, including by signposting, appropriate 'Protect advice'.
- If vulnerability is such that the victim needs support from other agencies inform the victim that they will be referred to them.
- Follow-up Regardless of action being undertaken by the responsible force Action Fraud will continue to inform victims whether their crime has been disseminated, disrupted or retain for intelligence

value at or by 28 days of reporting. Where а crime has been disseminated NFIB will share the details investigating of and responsible forces. Investigating forces will update responsible forces when necessary in line with the victim code of practice (eventhough technically this may not the NFIB apply). Under IT modernisation programme it may be possible for this to be done through common crime а management database available to all forces and NFIB. Where victim vulnerability makes it appropriate the responsible force will provide further support either directly or commissioning through the of outsourced services. The aims of such follow-up action may include:

- Supporting the victim with the emotional impact of the crime
- Assisting the victim in securing the information to begin any restorative action.
- Supporting the victim through any judicial process
- Guiding the victim in dealing with the financial impact of fraud

- Helping the victim safely
 restore their online identity
- Providing tailored crime prevention advice (available through the National Economic Crime Prevention Centre)
- **Conclude** The conclude phase sees the responsible force ensuring that victim needs have been met and that they have been made aware of the final outcome of their case. It is the intention that policing's support to victims will be reviewed and improved in line with victim feedback and the national Police Coordinator for Economic will Crime commission the appropriate surveys and feedback mechanisms for this.

VULNERABILITY

Purpose Key to policing delivering an effective and affordable service to victims is the tailoring of support to match need. A guide to victim need will be provided by NFIB through the Vulnerability Status included in the notification to forces of a victim in their area.

Vulnerability Criteria In the context of victims of fraud 'Vulnerability' should be seen as including, but not being

limited to, the general Home Office definition. Considerable work is being undertaken within academia, the Home Office and policing to better understand and define vulnerability but it is likely to include:

- The financial impact on quality of life for the victim (eg relative monetary value to the victim rather than absolute figure)
- The emotional impact
- The likelihood of the victim being repeatedly targeted

How Assessed Initial assessment of vulnerability will be undertaken at Action Fraud / NFIB. This will be a largely automated process based on the answers provided when victims report either on line or through the Action Fraud call centre. The Economic Crime Victim Care Unit project conducted in London at the beginning of 2015 identified a number of indicators of vulnerability, these will be developed further. It is intended that further shading can be provided by overlaying national and local victimology data on the individual cases. This would enable forces to be informed for example that whilst an individual may not currently be a victim their repeat demography, location and the type of fraud to which they have fallen victim makes them more vulnerable to repeat victimisation. The vulnerability status attached to a victim by NFIB is an initial guide and the responsible force will confirm or amend it at first contact with the victim and subsequently. A vulnerability status model might take the form illustrated in the table below:

Table 1: Indicative Vulnerability Status Model

STATUS	DEFINITION
VS1	Not a repeat victim and no indication of particular vulnerability.
	The reported crime has had limited financial or emotional impact.
	Not particularly likely to be a repeat victim. Most victims will fall
	into this category.
VS2	A repeat victim or likely to be a subject of repeat victimisation.
	The reported crime has, however, had limited financial or
	emotional impact.
VS3	The victim has experienced significant financial or emotional
	impact but has the capacity to self-help to a large extent.
VS4	The victim has experienced significant financial or emotional
	impact and is unable to recover from the crime without
	considerable support.

TailoredResponseThelocalresponse to victims will be guided bythe vulnerability status and deliveredaccording to local policy. In some forceareas the entirety of victim care will beprovided 'in house' while others mayoutsourceitcompletely.It

anticipated that most forces will conduct first contact themselves and then contract-out follow-up support where the victim needs it. Likely responses are suggested in Table 2 below:

Table 2: Indicative Response Model

STATUS	LIKELY RESPONSE
VS1	'1st Contact' by phone. Updates as case progresses.
VS2	^{(1st} Contact by personal visit. Ensure victim understands how they became a repeat victim and provision of appropriate prevention advice (normally through 'signposting' or generic prevention material).
VS3	'1 st Contact' by personal visit. Signposting to appropriate agencies and sources of support. Follow-up visit to check progress
VS4	^{(1st} Contact' by personal visit. Referral for specialist support (eg appropriate financial advice, charities, local authority, victim support organisation etc)

FURTHER DEVELOPMENT

The detail required to put this strategy into practice will be developed nationally by Policing's Crime Business Area through the working groups of the Economic Crime Portfolio. There will be wide consultation with relevant national agencies and other areas of policing.

Local forces and Police and Crime Commissioners will, of course, continue to develop their own local response, guided by the strategy.

SUPPORTING THE VICTIMS OF FRAUD – ACADEMIC STUDY

Introduction This short paper was developed by the National Fraud Academy drawing on previous academic research into the nature of fraud victimology. Further academic research into the nature of fraud victims and the appropriate response to their needs has been commissioned by the City of London.

Are fraud victims any different from victims of other crimes?

Most people would refer to fraud as simply a theft committed through trickery or deceit. Although this may be correct when considering the application of the law and the classification or typology of the offence, it would be wholly inappropriate to consider this classification when devising an effective strategy to support victims. In this regard the response provided to victims is often misdirected by not taking time to understand the methodology used in the commission of the fraud.

From a modus operandi perspective, rather than comparing fraud to theft, a more appropriate comparison may be violent and predatory offending. By analysing and comparing the criminal methodologies, certain 'cyber savvy' predatory offenders will assume a false identity and then use it to create a false online profile. Using this profile, they then identify potential targets, engaging with them, building trust, grooming them through a process of social engineering until sufficient trust has been built to follow through with the criminal act. When the target is finally victimised, this is not the end of the criminal conduct, the offender will often have other targets at various stages of the social engineering spectrum in preparation for victimisation.

This form of predatory offending is classified as a 'live crime', where the threat of harm is ongoing; it does not end with the first victim. By understanding the criminal methodology used by these offenders it is possible to draw parallels with many different fraud types, in particular, those committed via the internet, and, similarly, it is possible to understand how victims are selected, drawn in and eventually victimised.

As detailed above, it is not just the crime itself that must be considered, it is the complete lifecycle of communication and interaction between the victim and the suspect. Without this, the methodology used in committing the fraud cannot be properly understood and the victim cannot be provided with the correct support.

This concept is not just applicable to offences committed online, but is equally applicable to offences committed face to face or by the use of telephony. Through a study of the recent rise in Mandate Fraud it has been shown that the 'victim' is contacted an average of 5 times by the fraudster before a request is made to pay monies in a new (fraudsters) account, Jones (2014). Like other predatory offenders,

the fraudster is using social engineering on the victim, building a trust based relationship that will ultimately enable the commission of the offence.

There have been many studies by criminologists and psychologists examining the offending behaviour of predatory offenders; these studies haven't been limited to the final act of the crime, of equal importance has been the study of the predatory phase. To better understand the motives and modus operandi of the fraudster it is also necessary to focus on the entire lifecycle of their behaviour. From a victim perspective, it may be that more psychological harm is caused from the period of social engineering than from the commission of the fraud and the subsequent financial loss.

Many would argue that the harm from predatory and violent crimes is far greater than that of fraud but, according to early research by Ganzini et al (1990), which compared victims of fraud with those of violent crime, found that many were afflicted with depression as a consequence. Deem (2000) found that, to some, the effects of fraud can be comparable to that of having been subjected to serious violent crimes. A further study which looked into the impact of Robert Maxwell's pension fraud, Spalek (1999) identified anxiety, stress, fear and depression as being common emotional reactions. The study also found that a number of deaths were considered premature as a result of the fraud.

Although some may not consider it appropriate to classify fraud in the same context as predatory and violent crime, at the very least it should be viewed as a trust based crime, one of social engineering committed by predatory offenders who abuse victims without compassion or mercy.

Comparing the effects of fraud with violent crime

In the study of victims of fraud, Ganzini et al (1990) compared the emotional and physiological impact of fraud and violent crime on victims, including the statistical risk of victimisation. In the study twenty-nine percent of the victims of fraud experienced a major depressive episode in the first 20 months after their loss. Five victims (out of 77) developed suicidal tendencies after the loss and generalised anxiety disorder was found in 45% of the victims.

Ganzini (ibid) concluded that after violent victimisation, adequate social support is an important predictor of good recovery and release of psychiatric symptoms. Support for victims of fraud on the other hand, is less structured; criminologists have noted that victims of fraud are at greater risk of continued victimisation due to the 'trust' based nature of their crimes.

Although the above study was focussed on victims in the United States, a similar study was conducted looking at victims of the Maxwell pension fraud, Spalek (1999).

The research confirmed the findings of Ganzini, stating that the harms caused by corporate fraud are equivalent to, and often more devastating than those usually focused on by the criminal justice system. Victims of corporate fraud express a range of emotional and health problems, in addition to suffering from long-term financial difficulties.

In the largest study of fraud victims in England and Wales, Button et al (2012) examined the wide ranging effects these crimes have on victims, including broken relationships, deterioration of physical and mental health, attempts at suicide as well as some secondary impacts related to reputation and changes in behaviour. The research demonstrated that fraud victims share many characteristics with other victims of crime and yet services provided to support them are not as comprehensive or representative of the true harm.

How is vulnerability of fraud victims classified?

Under the Victims' Code, a vulnerable victim is classified as:

- Anyone under the age of 18 at the time of the offence.
- Anyone who is suffering from a mental disorder within the meaning of the Mental Health Act 1983.
- Those with a significant impairment of intelligence and social functioning.
- Those with a physical disability or who suffer from a mental disorder

The approach taken with the Victims' Code is one of support and service post event, after the crime has happened. The Code does not provide a means by which vulnerability can be identified and proactively used to prevent crime or further crimes against the same individual.

In the context of victims of fraud, vulnerability is not fixed or static, and contrary to popular misconceptions it is not reliant on an individual's age or their physical or mental capabilities. Rather, it is dynamic, triggered by a combination of circumstances, situations and external influences. Criminals behind some of the most successful frauds will often target individuals based on an assessment of their vulnerability to a particular approach or pitch.

By understanding how an individual's situation or circumstances could contribute towards their vulnerability, regardless of the age, capacity or capability of that person, a more informed victim focussed intervention is possible. Situations affecting an individual's vulnerability could range from a loss of income or being on a low income, becoming a carer, living in a particular area or without internet access.

Recognising that vulnerability is not necessarily permanent and that an individual's vulnerability is dynamic, it is possible to focus on the triggers that have contributed

towards the vulnerable state, such as a significant emotional event, e.g. bereavement, serious illness, divorce or redundancy.

For consumers, which many volume fraud victims are, vulnerability can vary depending on what services or products are being purchased, and how or by what method of communication the transaction is being conducted through.

It is not uncommon when an individual is susceptible to a particular vulnerability for this to lead to others, compounding their situation and their vulnerability. For example, individuals with low basic skills are also more likely to be unemployed (e.g. vulnerable to employment frauds), carers often suffer from ill-health and/or unemployment (e.g. vulnerable to health & support frauds); the elderly are at a greater risk of suffering from a recent bereavement and long-term illness (e.g. vulnerable to relationship & support frauds).

Vulnerability should not be seen as 'once classified', always vulnerable; the vulnerability should be viewed as unique in relation to the period of time when the classification was made. However, these vulnerabilities may very well indicate a predisposition to the susceptibility of becoming a repeat victim.

Victims of fraud should always be recognised as individuals first and classified in relation to their vulnerability second. This does not negate the need for timely interventions when individuals are recognised as being vulnerable, but it does ensure that they treated with respect and dignity as an individual, not as a generic 'vulnerable victim'.

Example:

A victim of a house burglary may be vulnerable, due to circumstances, of a secondary occurrence as criminals know that the goods stolen will more often than not be replaced following an insurance claim. In the same way, a victim of an investment fraud may be vulnerable to further crimes committed under the guise of 'fraud recovery' scams.

Returning to the concept of the victim of a house burglary, the main thrust of the 'police' support is a focus on weaknesses with the physical security that may need attention in order to prevent further offences. Limited consideration, from a police perspective, is given to the psychological impact of being burgled, the sense of violation, not feeling safe. For some the impact is so great that they see no option but to move. For victims of fraud, the impact can be just as severe, and for some, the need to distance themselves from the source of the crime, especially when it is committed online, can result in them withdrawing or being excluded from the digital marketplace.

Applying victim needs to support for victims

When considering crimes of fraud, it is not uncommon for the first thing a person considers is 'how much did they lose', unfortunately, the same mindset can often be applied to those providing support to victims fraud. Dealing with the purely 'financial' aspects of a fraud can leave victims emotionally and psychologically vulnerable.

Clearly, not all victims of fraud fit into this category, for victims of high volume low value frauds, such as online shopping or auction frauds, the psychological impact can be minimal and the primary concern of the victim is access to information and updates on the progress of their crime report, services which can be automated and provided through a range of new and emerging technologies.

Victims of the more serious crimes, those causing the most harm, are more often than not 'dynamically' vulnerable and at greater risk from the long term negative effects of the crime. For this group, the needs are complex and unique to each individual; to provide a service that is effective and affordable will require creative and flexible solutions.

Case Study: Senior Busters- Canadian Anti-Fraud Centre (CAFC)

The CAFC was one of the international forerunners (formed in 1991) for providing a centralized 'national' fraud reporting centre together with support for the victims of fraud, a model mirrored by Action Fraud and the NFIB. CAFC identified that seniors are targeted for many reasons: loneliness, lack of family support, age vulnerability and for health-related reasons such as Alzheimer's.

Seniors are particularly susceptible to fraud schemes because their generation tends to be more trusting and less likely to end conversations. Fraudulent telemarketers build relationships with seniors and gain their trust before victimising them. Ruined family lives, great financial losses and suicides have resulted from this brutal crime against the elderly.

Staff at the CAFC found they had neither the time nor the resources to follow up with victimised seniors so the Centre enlisted volunteer seniors who could help with the battle against mass marketing and identity fraud. The volunteers are able to relate personal experiences, provide support and establish rapport with elderly victims. The "seniors helping seniors" program was named SeniorBusters.

SeniorBusters was officially launched in October 1997, since then, it has grown to a group of approximately 50 active volunteers. They come from diverse backgrounds and bring many different skills to the CAFC and its attempt to reduce the level of mass marketing fraud and identity theft. This is clearly a successful and effective long-term strategy in reducing the number of seniors victimised by fraud. SeniorBusters helps fraud victims by:

- Relating personal experiences, wisdom and expertise
- Providing strength to victims
- Providing emotional and moral support
- Being sensitive to the needs of seniors
- Contacting victims as often as needed
- Educating and re-educating seniors
- Obtaining suspect company information
- Referring victims to other appropriate agencies
- Developing personal relationships with victims
- Ensuring that seniors have a place to turn to when they need assistance
- Helping victimised seniors regain personal dignity.

Current system for supporting victims of fraud

It should be noted that the support for victims of fraud is better now than it has ever been. Under the late National Fraud Authority considerable progress was made under the remit of 'Fighting Fraud Together' and with the development of the 'National Fraud Segmentation. Victim Support has invested in the training of staff and Action Fraud automatically refers victims to Victim Support and provides a wealth of support and advice through their website and call centre staff.

Through Action Fraud and the NFIB an Economic Crime Victims Unit is being piloted (London region) to provide additional support to victims who may be considered as vulnerable. A key deliverable from this pilot will be an informed picture of the potential levels of vulnerability from those crimes reported to Action Fraud, whether the system recognised them as vulnerable, if not, what could be done to ensure that those who are vulnerable are identified and provided with the appropriate support.

The pilot has already confirmed that vulnerability following a fraud, or to further offences of fraud, cannot be viewed in the same context as the Victims Code; what is required is a multi-dimensional matrix taking into account victim demographics, fraud methodologies, together with past, present and future triggers of individual vulnerability.

Additionally, the pilot has shown that victims own assessment of their vulnerability is not always the most reliable indicator; individuals can be blind or dismissive of their own vulnerabilities, an issue that fraudsters rely on and frequently take advantage of.

The majority of the services available could be viewed as 'reactive', providing generic support and guidance; without understanding or being able to assess dynamic vulnerability, these services could miss the triggers necessary to prevent a victim from becoming more vulnerable and susceptible to further victimisation.

Although there may be duplication and potential areas of conflict, none of the services or functions are wrong, they are doing a great job in providing support in one of the most challenging areas of modern day victimisation. Just as Action Fraud standardised and improved the fraud reporting process on behalf of England and Wales, so too is the potential for a centralised or nationally coordinated support service for victims of fraud.

The service however, should not be seen as one size fits all, but a structured matrix or menu of services and support tailored for the needs and vulnerabilities of individuals, groups and communities. The structure could follow the below structure:

Back End - Action Fraud: Rules based victim vulnerability assessment – identifying triggers which access or direct individuals to different support systems.

Fraud Victim Care Unit: Focussed on follow up contact with individuals identified by Action Fraud as 'Vulnerable' from either the original offence or to further offences. This unit is not to be considered as the final solution, but more of a psychological triage unit that identifies, classifies and transitions victims to the appropriate support systems.

Victim Support: Either contracted out or in-house, with specialist training to recognise the psychological trauma associated with fraud, together with the financial impact, able to provide effective first line support and where necessary, refer victims to professional support services.

Front End – Action Fraud: Generic fraud prevention and 'what to do' advice for those seeking to prevent or report fraud but not necessarily affected by it necessitating specialist support. Through the delivery of the 'next generation' combined NFIB and Action Fraud solution, it will be possible for victims to remotely access details and updates on their fraud reports, providing accessible support for low impact / low harm victims whose primary concern is knowing how or if their case is progressing.

Volunteers: Multi-tiered approach, working at both national and local levels.

Specials – developing a cadre of trained officers whose time is used providing support to victims where there knowledge of the community can be used to recognise and proactively provide support to groups that are, or may be targeted by fraudsters.

Busters – building on the Canadian model of 'Senior Busters' a more comprehensive network of support could be provided, not just for seniors but also including 'junior busters' for example, supporting a group of the community that may be cyber wise, but at the same time, vulnerable to fraud through a lack of being street wise.

For the above to be effective the focus of the support for victims of fraud must combine what we already know about the 'who' (victim demographics) with a more comprehensive understanding of the 'how' and 'why' (fraud methodology).

To make this work there is benefit in considering how current systems and national structures can be leveraged to best effect. By bringing together the intelligence from NFIB and Action Fraud with a permanent centralised victim triage / assessment unit (such as the pilot Economic Crime Victims Unit), together with the specialist support services detailed above, a nationally coordinated service can be provided to victims of fraud to a standard that has not been seen before.