Are vulnerable victims of fraud being identified and protected by public and private sector fraud investigators?

Matthew Newell

University of Portsmouth
Institute of Criminal Justice Studies

August 2019

Dissertation submitted in partial fulfilment for the requirements of the MSc Counter Fraud, Counter Corruption & Victimology degree

Are vulnerable victims of fraud being identified and protected by public and private sector fraud investigators?

Matthew Newell (878163)

August 2019

Supervisor – Jacki Tapley

Word Count – 14,518

Dissertation submitted in partial fulfilment for the requirements of the MSc Counter Fraud, Counter Corruption & Victimology degree

UNIVERSITY OF PORTSMOUTH
INSTITUTE OF CRIMINAL JUSTICE STUDIES

- I hereby declare that this dissertation is substantially my own work;
- I do consent to my dissertation in this attributed format (not anonymous), subject to final approval by the Board of Examiners, being made available electronically in the Library Dissertation Repository and/or the Department's digital repositories. Dissertations will normally be kept for a maximum of ten years;
- I understand that if I consent, this dissertation will be accessible only to staff and students for reference only;
- This permission may be revoked at any time by e-mailing data-protection@port.ac.uk.

SIGNED:

PRINT NAME: **M. NEWELL**

DATE: **18/08/2019**

ABSTRACT

This dissertation investigates how vulnerable victims are fraud are being identified and protected by organisations involved in fraud investigation. Primary research is conducted through the use of online questionnaires, with organisations in the public and private sectors invited to participate. The aim of this was to identify a ‘best practice’ approach to the identification of vulnerability and how to protect those identified. It was also aimed at identifying improvements to the current ways of working to ensure a better overall experience for victims.

Due to a low response rate there are great limitations to the research, exacerbated by all responses coming from Police forces only. There is therefore an emphasis placed on the analysis of the results in comparison to compliance with victim legislation, such as the Victims Code of Practice, and recent literature in the area, such as the HMICFRS reports. The research shows that there is still a disjointed approach to identifying vulnerable victims, with different definitions being used and different methods to evaluate it. Having said that, it is clear that all forces have developed a procedure in this area and place a great importance on it. There also appears to be a mixed approach to supporting victims. Education is placed at the forefront of thinking, with partnership working taking much of the pressure of forces. Respondents were also keen to improve their efforts in disrupting offenders and bringing them to justice, with a reminder that whilst victim focus is important, tacking offenders is one of the most effective ways in preventing victimisation. The research also found that practitioners are keen to share information with other organisations, but feel a lack of knowledge amongst those responsible breeds an incorrect fear of facing repercussions for unlawful sharing.

TABLE OF CONTENTS

INTRODUCTION

Fraud has become one of the most common crimes occurring in the UK (Evans, 2017) and now costs the UK economy around £190bn a year (Mothershaw, 2017). This growth has come about during times of austerity for investigative bodies, increasing global mobility and technological developments facilitating the commission of fraud and ability to avoid detection. As a result, practitioners are faced with seeking alternative tactics and methods to tackle the issue, as historical ways of policing are now no longer effective. The old adage of 'prevention is better than cure' is coming to the forefront of this thinking.

It is also important to understand that many victims of fraud get little or no service. Action Fraud is the national reporting centre for fraud and cyber offences and is the centralised hub that collates reports. The National Fraud Intelligence Bureau sits alongside this, processing intelligence and identifying emerging trends. The scale of fraud means that around 75% of reports are not investigated and are closed at source (Robins 2018). When this is put in to context against other crimes, it is a concerning thought as fraud and cyber-crime equate to almost half of all crime in England and Wales, a total of 5.2 millions offences, but only a quarter of victims will see their crime investigated (Blakeborough & Correia 2018).

Button et al (2009, page 6) defines fraud in a concise but accurate way;

"Fraud encompasses a wide range of behaviours that are linked by trickery or deceit with the intention it will culminate in some form of gain"

In practice the offender does not have to make a gain, as the Fraud Act 2006, allows for the offender to cause loss to another, or simply expose another to a risk of a loss. In reality however, this may be nothing more than ensuring any legal loopholes are tied up as in almost all of the cases, those who commit fraud will want a reward for their deceit.

There are multiple ways fraud can be committed. A quick review of the National Fraud & Cyber Crime reporting centre's website, Action Fraud (Action Fraud 2019), highlights up to 56 different types of fraud. These range from financial investments to doorstep scams, but all involve a dishonest element. Lying about the value of work to be carried out on your house, abusing your level of trust as a financial advisor to get a client to invest in a fake scheme to earn money, selling items on eBay that you don't own are but just a few examples.

All frauds can have an emotional as well as financial impact on the victim. This is particularly pertinent in romance frauds, where the victim is manipulated into believing they are in a relationship with the offender. Not only are they duped in to sending money to the offender, they are then left isolated and lonely as the person they fell in love with is simply a lie, with many left feeling emotionally scarred and contemplating suicide (BBC 2018). These victims are not only targeted because they are lonely and vulnerable, but are left even more so after the crime. These are the victims that this research aims to protect.

Conversely, investment frauds can also leave victims feeling emotionally damaged, although the embarrassment prevents them from reporting. Investment frauds can often target the wealthy as they promise large returns on large investments. The victims of such frauds can often be overlooked and not accepted as 'they can afford to lose the money' or 'should have known better'. This can prevent the victims from accepting their victim status and hiding what happened to them. If the money lost was for the victim's retirement or enjoyment in later life then they can suffer the same emotional distress as a romance victim (National Post 2017).

Both of these frauds may have a wide spectrum of victims which may not fit nicely into a single definition of a fraud victim but are ultimately vulnerable. This is the challenge facing fraud investigators and what this research hopes to try and understand further.

Alongside the drive for new investigative techniques there has also been a growing expectation of the Government to protect those most vulnerable in society. This has seen new laws covering hate crimes and local government acts such as the Care Act 2014 setting out relevant legal frameworks to protect adults at risk of abuse (Social Care Institute for Excellence 2016). There have also been improvements in the support provided to vulnerable victims throughout the Criminal Justice system. For example, the development of special measures has been vital in improving evidence in court, with better identification and support of victims improving such a service (Hamlyn et al 2004).

There is a key need to protect the most vulnerable in society. This research study will focus on vulnerable victims of fraud in an attempt to establish a 'best practice' for investigators who operate in this line of work.

This research does not set out to define what makes a victim vulnerable through any empirical analysis. It is designed to collate what each investigator defines as a vulnerable victim in their own organisation in the hope of identifying patterns or similar characteristics between the definitions. It will then seek to identify how different investigators use this data to protect current victims and feed this back into preventing future victims. This prevention work will be invaluable for organisations in moving forward and being efficient with the resources they have.

Fraud is not simply a problem to be tackled by one individual organisation alone. It is one which must be tackled collectively through the pooling of resources, intelligence and powers of multiple bodies, as shown through the creation of the National Economic Crime Centre (NCA 2019). Therefore, this research will touch on how investigators can share relevant data to protect vulnerable victims together. Due to the benefits it could have on society it is hoped that a multitude of organisations will be willing to share ideas on how they could all work in collaboration to better protect society together.

AIMS

- To critically assess how organisations involved in fraud investigation identify and protect vulnerable victims of fraud by examining their policies and processes.
- To identify if current techniques require improvement, and if so how practitioners feel this could be achieved.
- To identify possible prevention strategies to protect vulnerable people and reduce the risk of harm.

OBJECTIVES

To collect primary data to compare how public and private organisations involved in fraud investigation;

A) Define and identify vulnerable victims

B) Identify what they do with this data (if they do actually record such data), how they record it and how they use it, i.e. how they protect their vulnerable victims

C) Examine how these organisations can share data to improve their identification of vulnerability and develop prevention strategies.

LITERATURE REVIEW

There has been a great deal of development in area of victimology over the last 80 years or so, developing the initial positivist theories of Wolfgang and ‘victim participation’ (Wolfgang 1957) and realising that there a multitude of factors involved and that ultimately, the victim should always be at the forefront of thinking.

The ‘victim’, and victimology, has clearly been influenced by significant events, society, politics and the media. Despite the developments in victimology and the emerging theories, the positivist undertone is one that is hard to shake. Rock’s (2018) notion of victim foolishness, or the ‘risky lifestyle’ (Davies 2017), can often be a comforting thought to society as everyone wants to feel in control of their own life and be free from risk (Walklate 2007). The belief that we can avoid this risky path and be in control of our potential victimisation helps us feel safer. The media re-emphasises the message as crime stories apportioning blame on others, typically on institutions, sustain considerable public interest over the innocent person being victimised (Greer 2017).

Examining the victimology of fraud is a near impossible task. As Button et al (2009) identifies, there are numerous types of frauds and therefore numerous types of victims, making any generalisations extremely difficult. There is also sadly very little acceptance of fraud victims in society, with them often being labelled stupid, gullible or greedy. Even the Chief Commissioner of the Metropolitan Police stated, in 2016, that victims of online fraud who were receiving compensation from banks were “being rewarded for bad behaviour” (Grierson 2016). Even worse, many people argue that fraud is a ‘victimless’ crime’ (Button et al 2014), with individual victims being compensated or large companies just being able to absorb the losses. There is still such a strong stigma around being the victim of fraud that many suffer in silence due to a feeling of shame around what they have done (Cross 2016). This feeling of being at fault is still very much the starting position for many victims of fraud. Victims of romance fraud feel they were stupid and should have known better, or victims of investment fraud are labelled ‘greedy’ or ‘stupid’ and put themselves into chasing a deal that was too good to be true (Button et al 2009). This simply reemphasises the early ‘positivist’ theories that the victim was involved in their own victimisation. These notions have undoubtedly hindered the progress of victimology in fraud and caused there to be little acceptance of them as victims.

To compound this, victims are then further victimised when trying to obtain justice. They face inadequacies in the state’s response to fraud Cross (2016), for example being told it is a civil issue, or many are actually are told they are to blame by their banks and refused compensation (Greaves 2018). There is clearly some acceptance that a proportion of fraud victims are deserving of help and that they didn’t become victims due to their own participation, but this appears to be the exception to the rule. Society needs educating to the process of fraud victimisation before they will truly understand how deserving they are of support.

It is clear the developments in victimology have improved the knowledge and understanding of victims in certain crime types, such as rape, but it is becoming clearer that there can never be a utopian victimology theory. Not only are there differences in how different crimes affect people, each victim of victims of the same crime may react to their victimisation in their own unique way (Walklate 2017). Fraud could still be classed as a relatively new crime, with the main legislation, the Fraud Act 2006, only coming into power in January 2007. Coupled with the rise of the internet and most fraud now being cyber enabled, society have had little time to understand the victimisation of fraud victims. It can therefore be said that studies, like this one, are key in developing the understanding of victimisation in fraud and promoting support and protection.

The importance of protecting the interests of those victims most vulnerable in society has steadily grown over the last few decades, with the first giant leap coming in the form of the Youth Justice and Criminal Evidence Act 1999. This was aimed at vulnerable and intimidated witnesses and brought together a collection of special measures that helped them provide their best evidence to the court (Macpherson 2001). This meant previously unheard witnesses could now come forward to provide evidence, achieving justice for themselves or assisting others. This legislation also provided a clear definition of a vulnerable witness;

- All child witnesses (under 18)
- Any witness whose quality of evidence is likely to be diminished because they:
  - are suffering from a mental disorder; or
  - have a significant impairment of intelligence and social functioning; or
  - have a physical disability or are suffering from a physical disorder.

(CPS 2019)

This is a very broad definition deliberately designed to encompass all who may require such assistance.

Further developments came with the Victims Code of Practice in 2006, setting out key rights of victims in the whole criminal justice process (Victim Support 2019). This further emphasised the rights of vulnerable victims to enhanced support and set out the key information and support all victims should be provided with. It also ensured that almost all government organisations adhered to providing the same level of service (Ministry of Justice 2015).

The private sector has been included in this research as they are not bound by such legislation. It is hoped that the research will identify if they uphold the spirit of the Victims Code, whether they have developed their own policies around victim care, or whether they ignore it all together. As noted earlier, there have been great strides in the development of victim care but there might still be lessons to be learnt from the private sector. Conversely, it might identify a large difference in approaches and something for the private sector to develop.

Even as recently as September 2018 the Government released its Victim Strategy, setting out further new measures and its desire to put in place the relevant legislation to ensure the new guidelines are followed (HM Government 2018). This strategy sets out how it wants to improve services for victims, including increasing the number of intermediaries for vulnerable victims, increase the use of video links so vulnerable victims can present their evidence to court in a way more suited to their needs and improve victim contact (HM Government 2018).

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) assess the effectiveness of Police Forces in the UK and ensure they maintain high standards of serving the public. They regularly assess the effectiveness of forces to protect vulnerable victims and promote the THRIVE process (HMICFRS 2018). This is a risk based assessment covering Threat, Harm, Risk and Engage (Smith & Swann 2016 page 4). The definition used here for vulnerability is;

"A person is vulnerable if as a result of their situation or circumstances, they are unable to take care or protect themselves, or others, from harm or exploitation"

Again, this is a very subjective definition of vulnerability, allowing the decision maker freedom to interpret it how they feel. There is a deliberate steer away from setting set criteria, for example they must be over 60, have mental health issues etc. The element of being able to take care of yourself is a key concept in this area. When we think of those most vulnerable to us, we will subconsciously make this type of assessment and are likely to find this to be a major factor.

However, this flexibility for a subjective assessment may also allow pitfalls in the process. For example, in the THRIVE example above, someone may be able to cook and clean and take care of themselves in that sense, but may be overly trusting and believe the word of a stranger, making them very vulnerable in another. An inexperienced assessor may not explore these differences and simply look at the criteria in a simple way. Having a set criterion will avoid this subjectivity and ensure a uniformed approach to risk assessing vulnerability.

This research does not set out to define what makes a victim vulnerable through any empirical analysis. It is designed to collate what each investigator defines as a vulnerable victim in their own organisation in the hope of identifying patterns or similar characteristics between the definitions in order to inform best practice. It will then seek to identify how different investigators use this data to protect current victims and feed this back into preventing future victims. This prevention work will be invaluable for organisations in moving forward and being efficient with the resources they have. The HMICFRS have already noted that forces are doing well in assessing vulnerability (HMIFRCS 2019), but as the fraudsters continue to evolve and improve, so should those tasked with bringing them to justice.

Whilst victims have seen a development in how they are treated, fraud has been steadily growing into the major crime type in the UK (Blakeborough & Correia 2018). It could be argued that it is still a relatively new crime, with the main legislation coming in the form of the Fraud Act 2006. This was a much needed addition to simplify prosecutions and make offences more straightforward for practitioners and juries to understand (Ministry of Justice 2012). In fact though, the first recorded fraud can be seen as far back as 360 BC. A ship owner planned to sink an empty ship but falsely claim on his insurance policy that it was fully laden (CIFAS 2019). This shows that unfortunately man has had the propensity to lie to make a gain for a long time, it is simply that the development of technology in the 21st century has accelerated the crime.

In 2005 the then Attorney General decided to launch a review into fraud amongst fears it was having a serious impact on the economy (Button et al 2008). This led to multiple recommendations, including the creation of a lead force, the City of London Police, and creation of a national reporting centre, what is now Action Fraud (Button et al 2008). It was only then that a real focus was placed on fraud and a strategic response created. It also highlighted the fact that victims of fraud were confused about where to report fraud and so a centralised reporting body helped make this clearer to victims (HMICFRS 2019a). Despite this being available to the public for several years now, there are still issues in victims of fraud understanding the right body to report their fraud to and obtaining enough interest in it to take further for investigation (Button et al 2009a).

Fraud is not simply a problem to be tackled by one individual organisation alone. It is one which must be tackled collectively through the pooling of resources, intelligence and powers of multiple bodies, as shown through the recent creation of the National Economic Crime Centre (FT.com, 2018). There is already some collaborative work ongoing between different organisations to protect victims (HMICFRS 2019a) including the new Joint Task Force combining law enforcement, the banking industry and the government (Home Office 2016).

This research will therefore touch on how investigators can share relevant data to protect vulnerable victims together. Due to the benefits it could have on society it is hoped that a multitude of organisations will be willing to share ideas on how they could all work in collaboration to better protect society together.

In line with the growing movement of prevention and disruption there have been multiple relevant studies in this area. Cross (2016) has examined an approach taken in Australia to identify individuals sending money to certain high risk countries and send them a series of warning letters educating them about the potential frauds they may be involved in. Research has shown that a significant number of people ceased sending money after Police intervention, therefore preventing further losses to themselves. This research helps highlight that shifting the focus onto victims can significantly help crime prevention.

Cross (2016) also highlights the importance of work in this area as aside from the financial impact of fraud, the emotional and psychological effects can be longer lasting and more severe, despite the poor response it is seeing from law enforcement currently. This shows the value in identifying vulnerable victims and working with them to prevent repeat victimisation.

Drew & Farrell (2018) also advocate the use of crime prevention techniques focusing on victims through education and awareness as the most effective way of tackling fraud. They point to the increasing difficulties faced by law enforcement with suspects ‘hiding’ in the internet and protected by jurisdictional borders and a lack of international co-operation. They also touch on a key area on underreporting due to the victim’s embarrassment or shame.

Work conducted by Sheibe et al (2014 p.278) also sets out the value this research can have. It concluded that “forewarning can effectively reduce fraud susceptibility in vulnerable consumers”. Although this study mainly focused on elderly American victims it clearly shows that through identification and prevention techniques, fraud can be prevented.

In fact, age can play a key part in vulnerability in itself. There are numerous articles in support of this, such as Reisig & Holtfreter (2013), who even go as far as highlighting it is the over 60’s who are most vulnerable. Research conducted by Age UK (2015) suggested that over half of people aged 65 and over had been targeted by fraudsters. Clearly if they are being heavily targeted by offenders, then offenders have identified that there is some value in targeting them.

This brings up an interesting question regarding vulnerability and age. Button et al (2009) is keen to correct the misconception that the elderly are by far the most likely to be victims of fraud. He also refers to various studies finding that due to the wide nature of fraud there are often times where a younger demographic are most susceptible. This shows the wide nature of fraud and the changing nature of victimisation within it. This is where this research will seek to identify how, or if, organisations take this consideration on board in identifying vulnerability and how their processes may overcome it. It will identify in organisations in the UK place an age marker on vulnerability and if so at what age, allowing for future discussion. This research will not examine whether it is right or wrong to set an age, but merely look to identify what organisations may set it at and identify their reasons for doing so.

Sussex Police are the UK Police Force that introduced the now nationally adopted “Operation SIGNATURE” (Sussex Police 2018). This puts in place processes that allow the Police force to identify and protect vulnerable victims, linking them in with other support services. It was created to provide an extra layer of support to victims and prevent those most vulnerable in society to suffering repeat victimisation (HMICFRS 2019a). Little is known regarding the fine details of the programme, but it uses ‘vulnerability factors’, such as age, to identify potential vulnerable victims (HMICFRS 2019a). It is hoped that through this research the actual factors used will be identified so a comparison can be made across different sectors. If someone is identified as vulnerable then they are visited by a member of the police force and their particular needs are assessed to ensure the support measures are in place to prevent further victimisation (HMICRFS 2019a).

Shearlock & Cambridge (2009) discuss the safeguarding of vulnerable adults in one particular are of the UK, Somerset. Although much of the paper regards supporting victims through the court process and discusses crimes that are not fraud related, it shows the importance of cross agency working in protecting vulnerable victims. Through the use of multi-agency public protection arrangements (MAPPA) and multi-agency risk assessment conferences (MARAC) vital information can be shared. The police, social services, victim support, housing associations etc can all attend these meetings and share information. This highlights that multiple agencies can provide the best service to victims when working in collaboration. This research will look to see how those involved in fraud investigation can do something similar, with the hope of the success of the MARACs. For example, a female victim of a romance scam may mention their social worker that they have met someone online. This social worker can ask further questions to identify it is a scam and then share these details with the Police. They can then intervene, educating the female regarding the offence and investigating the offender. The Police can then share this information with the females GP who may be required to provide medical support if the victim is feeling depressed regarding the incident. This victim has therefore benefitted from the support services interacting with each other.

Conversely, collaborative working can cause confusion about who actually holds the responsibility for tackling the problem. Information can be shared on a particular victim of crime but then law enforcement may see it as a social care problem and social care see it as a crime for the police to deal with. Strict boundaries and responsibilities are required for collaborative work to be a success.

HMICFRS have recently reviewed how effective Police forces in the UK are in dealing with fraud (HMICFRS 2019a). One specific area they looked at was around the identification of vulnerable victims. They were satisfied with the work that call centre staff completed but noted that there were almost a quarter of a million online reports that were completed by the victim themselves (HMICFRS 2019a). Although online reports are keyword searched to try and rectify this, there still remains a heavy reliance on the victim to accurately state their impact levels in order for them to get the level of service they require. Again, although the report notes that some forces do review their own victim data which is made up of these victim reports, there still appears to be holes in the process through which said victims could fall through.

The same report also refers to ongoing work to support vulnerable victims of fraud. It refers to forces using Operation Signature as a guideline but also several forces trialling the use of the National Economic Crime Victim Care Unit (ECVCU) (HMICFRS 2019a). Although there is limited literature on the ECVCU it appears to be a care unit specifically aimed at victims of fraud, ensuring that relevant care is provided to all victims and any vulnerability identified and addressed (London.gov 2018). The HMICFRS (2019a) report does make it clear though, although these are seen as best practice models they have not necessarily been fully implemented or adopted by each force. They also admit their own limitations in pushing for a national standard that has not been truly audited and evaluated.

RESEARCH METHODS

METHODOLOGY

Research was conducted through the use of an online questionnaire to obtain primary data. Participants were given a set list of questions to answer, with many open questions included to allow more qualitative responses. The questionnaire was structured to ensure specific points were covered and made as clear as possible to ensure the respondent knew the type of answer that the questionnaire hoped to uncover. The list of questions asked can be found in Appendix B.

The final part of the questionnaire encouraged the participant to put forward ideas of how to work in collaboration. The responses were anticipated to be more generalized and almost theoretical.

The research was designed to take around 30 minutes to complete. This was done to try and encourage participation as it was felt a lengthy questionnaire would discourage participants who had to fit the survey into their busy working lives.

Conducting the research through the use of interviews was considered, as there are many benefits to engaging with people directly. However, issues with time and cost, not only in conducting the interviews but in analysing the data, meant that they were not viable. The speed and scope of an online questionnaire meant that this method was therefore chosen (Noaks & Wincup 2011). The same questions were ultimately asked of the respondent, whether it had been done through a questionnaire or interview.

The questionnaire was designed using a series of focused open and closed questions in order to achieve the best answers. They asked about a very specific topic or area of the research but as there were multiple possible answers the question remained open enough for each respondent to answer accordingly. This was done in order to maintain a general overall structure to the questionnaire but have room for flexibility. This aspect was vital in trying to achieve the final aim of the research.

The questionnaire was conducted using Bristol Online Survey. A traditional method of sending questionnaires via post was considered but due to multiple reasons it was discarded. Not only were there greater security risks involved, it would potentially slow the process down and risked the requests being lost in the internal dispatch of large organisations. By conducting the questionnaire online it made the process quicker and more efficient, going direct to the recipient and being returned within seconds of completion. There was also the possibility of sending it in the body of an email, or as an attachment, but it was felt that this does not portray a professional approach and may have still caused security concerns. If the attachments were to be password protected then it would have allowed greater security, but required extra effort on behalf of the participant and multiple phone calls to the researcher to provide the relevant passwords.

All results from the research was designed to be collated in two separate ways. Those relating to Aim (A) would allow quantifiable recording of results due to the potential for many investigators using similar criteria to identify vulnerable victims, e.g. age range, disability etc. A quantifiable method of collating these results was considered, but it was felt this might narrow down responses based on preconceived ideas and therefore not appropriate (McKim 2017). Aim (B) was anticipated to produce a mixture of quantifiable results with slight variables on certain initiatives on protecting the vulnerable. These results were therefore designed to be collated quantifiably, i.e. coded, but with extra initiatives highlighted alongside. For example, respondents may refer victims to certain support groups, or they may allocate a follow up visit. These could therefore be compared and quantified amongst respondents, e.g. 70% of respondents referred victims to victim support. Aim (C) was anticipated to produce a large amount of qualitative data for review, although it was thought that there might have been some common themes. These ideas were to be placed into individual case summaries and linked where similar ideas were outlined.

A formal email was sent out to them giving them the option to participate in the questionnaire under a completely voluntary basis. A strict deadline to complete the questionnaire was also included to ensure that the research was completed in time, although this was latterly extended slightly due to a low response rate.

RESEARCH PARTICIPANTS / SAMPLE

The participants identified for this research are organisations in the public or private sector who are involved in fraud investigations and who may come across vulnerable victims of crime in the course of such work. A full list of the organisations chosen can be found in Appendix A.

They were identified using a mixture of methods; the researcher’s personal knowledge, online research, and academic research, such as BUTTON et al (2009) mentioned earlier. As Relbanks (2018) highlights, there are over 300 banks and 45 building societies in the UK, a sample size unmanageable in this research task. As the banking sector plays a key part in protecting the vulnerable, the 26 largest UK high street and online banks were chosen to be included in the questionnaire (Gartside 2018). The rationale for this is that the largest banks will hold the greatest number of customers and so their processes will affect the highest percentage of vulnerable customers. Likewise, there are 44 Police Forces in England & Wales, including British Transport Police, and to include results from them all would not only be resource intensive, it could bias results towards the ways adopted by UK Police Forces only. Therefore, the forces were ranked by the number of officers they employ with the top and bottom 10 forces being selected for the questionnaire to try and gain a mixture of responses (Wikipedia 2019).

Other organisations that don't investigate but may come across such issues will also be invited to take part. It is felt that they may have a useful input into the matter and could help facilitate the sharing of data;

- Action Fraud
- CIFAS
- Experian
- Citizens advice
- Victim support

ETHICAL CONSIDERATIONS

A great deal of consideration was put into the ethical side of the research as the identification of vulnerability is a very subjective and personal topic. Some respondents may have been reluctant to identify their criteria for fear of repercussions by customers if they found out. They were reassured in their engagement letter that they will remain anonymous in the research and that the researcher would only hold details of those asked to participate or those who have since requested to be involved in interviews.

The organisations approached in the research were also the only subjects required to give consent to participate. For example, if Organisation 1 has recorded Mrs SMITH as vulnerable and the research required Mrs SMITH’s details then there would be further ethical considerations and subjects to obtain consent from. This research was simply asking Organisation 1 for the procedures and policies around identifying people as vulnerable (e.g. Mrs SMITH), hence the data holder was the only person required to consider who to approach for consent.

There was no anticipated harm to the subjects in this research as it was focused on procedures and protocols, not specific people, and no personal data was recorded.

None of the participants were being coerced into taking part and they all took part of their own free will. Due to the researcher being involved in the relevant field there are numerous contacts that have been made throughout the years. These were not exploited in any way to ‘force’ participation but enabled the questionnaires to be sent to the relevant people and departments. For example, an email sent to a generic email address of a bank may take several weeks until it reaches the relevant person who could answer the question. These contacts were made expressly aware that they were nothing more than ‘gatekeepers’, requested to disseminate the questionnaire only. No expectations were be placed on them to elicit a response. Having made all of this clear to the gatekeeper it is felt that any responses were truly voluntary only.

It was hoped that other investigators and organisations would be willing to take part in the research through a moral duty. It is thought that all investigators would share a common goal to protect the vulnerable and identify if there is something more that could be done.

It was identified that many organisations may be concerned about potential reputational harm in the sharing of data or may have concerns regarding the disclosure of the private tactics of law enforcement agencies. In these circumstances it was expected that they would not participate in the research as the need for confidentiality will outweigh the needs of the research. It was made clear from the start that they did not have to participate if they did not wish to, ensuring they did not feel pressured into consenting and disclosing information they did not want to.

It was not thought that the identification of what investigators class as a vulnerable person will affect security tactics. The information from this research will not aid offenders in anyway or alter their pattern of offending. For example, if vulnerable victims are classed as over 70 then offenders are not going to ignore this age bracket and target younger for example. The information of which organisations share data and which don't might be useful but again this research will not share this. It will simply highlight areas where different anonymous organisations feel it may be beneficial.

RESULTS & ANALYSIS OF THE RESEARCH

Issues arising from the research process

Unfortunately, despite the research being sent to a large number of potential participants, with a follow up request, only 3 responses were received. The research can therefore not be looked at as a representative sample, with all responses coming from Police forces, but will hopefully still show some insight into its aims.

The first clear issue for discussion is that all the responses came from Police services. The fact that the researcher works in law enforcement may well be an influence on their participation. This common ground may have fostered a level of trust and willingness to participate. Had the researcher been working in a different sector it may have encouraged further support from colleagues in that industry, if this same effect were to be replicated.

Several responses were received from different banks stating that due to customer confidentiality they weren't able to participate. This is disappointing as the survey was designed with this concern in mind. It was designed to be anonymous and focus on procedural matters rather than customers, and this was made clear in the literature provided to potential participants. It is perhaps not too surprising however in the current climate of data privacy, confidentiality and security that the potential participant chose the easier option of abstaining from the research.

If the research was to be conducted again, its literature would strongly make the point that such concerns had been considered and addressed, and include this early on in the invitation. Some potential participants may have made an early assessment of the research and not fully read the document. Another consideration would be around conducting the research in partnership with a trusted organisation in this field, such as Experian or CIFAS. As these organisations already have strong links with the different organisations chosen it would hopefully provide respondents with more confidence to participate.

A final consideration would be to change the methodology of the research. If trust was an issue for respondents then it might have been more effective to conduct the interviews in person, allowing a discussion around confidentiality and putting the respondent at ease. However, it is not felt though that this would have made a material difference to the response rate. Even if this method was chosen it would still require the willing participation of the respondent, with the added effort of corresponding with the researcher to facilitate a time, date location for the research to be conducted. Then, after this had been arranged, they would still hold the original concerns about sharing such data surrounding the way they supported their victims.

It may ultimately be that this was such an area of sensitivity that any non-judicial or organisational review would have failed to reach the required levels of support to make valid conclusions from.

The respondent progress chart has also been reviewed to identify if there could be some insight into the participants minds;

p.1	**p.2**	**p.3**	**p.4**	**p.5**	**p.6**
41	8	4	4	5	6

The survey recorded a total of 6 responses to the survey, although 3 of these were completely blank for whatever reason. There is a clear drop out from the first page of the study, with minimal amounts of participants going onto the other pages. Part of this however may have be accounted for by the researcher checking the link was working and hence only viewing the first page. This shows therefore that unfortunately there was a low take up on the research, with very little respondents actually deciding to review the questions on the research. The topic areas were already provided to potential participants in their invitation letter so in theory only those who would be willing to participate would have entered the survey.

Perhaps it was the first page itself that stopped participants from continuing further. Respondents had been assured with anonymity in their responses, but when they saw the first page requesting their sector of employment and title they may have been put off, feeling this would reveal too much about them. This was always going to be a sensitive area to draw a line with. If the question hadn't been asked then the survey could have been skewed by a sample only representing a certain sector. A perfect example can be seen in the results obtained in this survey – they are all from Police forces. Now we know that fact we can be more balanced in interpreting the results of the research, understanding that often Police forces link in with one another and share ideas and are ultimately governed by the same legislation and procedures. Without this information it may be felt that investigators on the whole operated in the same way, something which could be a complete fallacy. It was also felt it was important to gauge the role of the person responding. Someone working in this niche area, identifying vulnerability for their organisation may provide a 'full picture' of their organisations aims and methods, compared to a general investigator or call handler for example. Once the survey had reached the relevant organisations chosen for participation it was completely out of the researchers' hands as to where it would be sent and who would ultimately be asked to reply.

If the research were to be repeated then perhaps an explanation could be made on the reasons behind these questions, with an emphasis on them being voluntary if the participant still had concerns about disclosing such information. However, without feedback from those who commenced the questionnaire we will never know how much this was an influence in them ceasing their participation.

As the response rate was low and all responses came from the same sector, a thematic review of the responses will now be conducted. The key areas of the research centred around Assessment of Vulnerability, Protection of Victims and Improvement in the process. The assessment of the results will therefore be centred around these themes;

1. Assessment of Vulnerability

This is a key area for Police forces. The HMICFRS (2019a) have already highlighted that there is an inconsistent service provided due to the nature of how reports are taken. They note that fraud reporting is very unique in that it is one of the few occasions where victims record their own crime and so if they under evaluate the impact levels they may miss out on much needed support. The HMICFRS (2019a) report does highlight however that when reports are taken by call centre staff they usually receive a good service and identify relevant vulnerability.

As discussed earlier, the Police can draw upon definitions of vulnerability from the court process (CPS definition) or the recommended one from HMICFRS (2019a) in which they are assessed. Even in the limited responses there appears to be a difference in how the respondents approach the issue, with one choosing a more objective approach and setting out key parameters, whilst the other two adopt the subjective approach. The list of criteria provided by one respondent covers;

"Cultural sensitivities, disabilities, elderly, dementia, learning difficulties, family support, financial difficulties, suicide risk, self-harm, drug and alcohol dependencies, illness, repeat victim, bereavement, mental illness, domestic abuse"

Of the others, one respondent provided the definition discussed earlier under the THRIVE process (Smith, W. & Swann, J. (2016) and the other gave another subjective definition of;

"Vulnerability is those who are at risk of becoming victims due to their mental, physical or social circumstances"

Although the final respondent had a subjective definition of vulnerability, they then also used certain criteria to help in their assessment;

"Mental health issues, age, physical difficulties, repeat victims, crime type e.g. dating fraud, dependency i.e. drugs/ alcohol"

The results show that although all the respondents have a slightly different definition of vulnerability, they use a mixture of subjective and objective assessments. They may have a wide definition that allows flexibility in their assessment, but alongside this they have a set criterion of key areas for the assessor to consider when making their judgement. This appears to be a perfect balance between allowing the assessor the flexibility required, but giving clear and helpful guidance for those more inexperienced. Concerns may be raised however as to why all respondents didn't refer to the HMICFRS's definition, as this is what is regarded as the national standard. The answer to this question may be found when respondents were asked how they developed these definitions. Whilst one respondent stated that they had reviewed their fraud risk and linked in with best practice from the City of London Police, the lead force in this area of crime, another respondent stated;

"By gaining knowledge from others in this field, training, meeting, information gathering and experience with victims"

This highlights another key area in that there has to be a cyclical learning process in his field, in which techniques are tried and tested and continually improved on. This respondent has the confidence to develop their own techniques in assessing vulnerability based on the results they see. The HMICFRS (2019a) have admitted that the various schemes they are trying to champion as best practice have received little evaluation. It is therefore not surprising, and perhaps not a bad thing, that forces are forging forward in developing their own practices, as long as consideration is made around the many safeguards to the learning process that must be considered in order for it to be accurate, such as sample sizes and researcher bias etc. Hopefully these results are then fed back into the City of London and HMICFRS to ensure that this learning is shared.

One respondent concerningly stated they didn't know why they had adopted the definition provided. This raises real concerns about the procedures employed by this force as there should be a clear definition that is taught to all officers tasked with identifying vulnerability.

It is clear that fraud can affect a wide range of people throughout different times of their lives. BUTTON et al (2009 page 5) highlights the diversity of fraud offences and how "fraud does not attract one type of victim" and that "Men, women, the old and the young tend to fall for different variations". It is therefore important for organisations to remember this when considering definitions, as most respondents have done. They reflect that there is no one typology for a victim of 'fraud'. A large percentage of frauds will be targeted towards the elderly and overtly vulnerable, with over 80% of doorstep scam victims being elderly for example (HMICFRS 2019b). However, middle aged woman are often the main targets of romance fraud (Whitty 2018) and they are unlikely to be covered in the objective definition earlier. A romance fraud is where an offender uses the pretences of wanting to develop a relationship with a victim in order to extract money from them or use their bank accounts to launder money. Offenders exploit those wanting to date and find love in order to achieve their aims. These victims are far less likely to possess many of the characteristics described earlier. They are not suffering mental health problems, they are not typically elderly, they are not of unsound judgement etc. In fact, the average victim is female and 50 years old (Peachey 2019). However, once they have fallen victim to the fraud they become vulnerable to further losses as they hold onto the belief of a relationship or suffer extreme emotional heartache when they realise not only have they lost money to the scam, but they have also lost the partner they thought they had. It is therefore important to see that some of the definitions above specifically include romance fraud as a criteria for vulnerability or include that their social circumstances can be a factor.

All the results from the questionnaire refer to the victim as a person, looking at what traits a person has that makes them vulnerable. Not one respondent mentioned, or appears to consider, companies as vulnerable victims, an observation also noted by the HMICFRS (2019a). Whilst there may be little empathy shown towards large corporations who fall victim to fraud, no matter how big or small, there could be some key considerations for when small medium enterprises fall victim to such scams. Small firms are likely to lose twice as much to fraud as larger firms and naturally the impact of this will be far greater, even causing the business to collapse (Stockton 2018). The emotional effects a serious fraud could have on a business owner, threatening to destroy all they have worked for, is surely akin to an individual suffering a large loss of their savings? Why therefore should some business frauds be treated as if they were an individual going through the same mental health problems and be supported accordingly?

The questionnaire also examined how organisations identify vulnerability, looking at the processes they use and the data they consider.

The main theme appeared to be that they made an assessment through speaking to victims and asking open questions. If these people are suitably trained and have the skills to identify vulnerability then this is clearly an effective way of identifying vulnerability. The personal skills of the investigator being able to speak to someone, respond to their answers and delve deeper into their background can often be far more effective than simply going through a checklist. At the same time though they have a backup list of criteria to help justify their personal assessments as most respondents also used a risk matrix approach in considering vulnerability. Although it is not clear what the respondent's vulnerability matrix is, other than by referring to previous answers for indications, it is clear that they most respondents have a policy in place. This shows at least that in relation to the response's received all organisations were clearly aware of their need to have such a system in place to identify vulnerability.

One respondent also reviews previous incidents or interactions with the victim to help gauge their vulnerability. This again is highly effective where a victim may not be engaging with the investigator or finds it difficult to communicate. Victims can often respond to the same crime in a very different manner (Mythen & McGowan 2007) so a set list of questions or criteria could be limiting to identify how they have truly been affected. This also fits in with the THRIVE process and National Decision-Making Model that Police forces follow (Smith & Swann 2016). This intelligence gathering is the initial phase of making a decision on how to tackle the problem faced and be the basis to all decisions made by the police.

A rather worrying set of responses were received when participants were asked about what data sources they use to identify vulnerability. One respondent simply replied "conducting assessments" but even worse, one replied "unknown". As mentioned before, this could be down to the respondent’s personal lack of knowledge, but without gathering a clear picture of the issues faced by the victim how can an accurate assessment ever be made? It is somewhat shocking to hear that they have a very limited mindset in terms of where to find relevant information from to support with their assessment. This could be very detrimental to the process, simply replying on the information provided by the victim on this specific occasion. When research shows that the public are dissatisfied with the Police (Tapley 2005), then to simply rely on them to engage may be naïve. If victims don’t trust the police they are unlikely to provide the full picture. This problem is only exacerbated with vulnerable people, who often feel let down by the justice system (O’Hara 2015).

Fortunately, the final respondent’s answer showed a far more comprehensive use of data, utilising not only their own forces data but external data from other forces and other agencies. This holistic approach is suggestive of best practice, ensuring that all possible intelligence is gathered to improve the decision-making process. It is also the first sign in the questionnaire that collaborative work is ongoing to ensure vulnerable victims are identified. It must not be forgotten of course that this is the response from a public sector body and thus more likely to have access and share data with other public bodies in the same field. In reality though, does this really go far enough? As this research sought to identify, could there not be external sources who hold relevant data they could share with other organisations? As Button et al (2009a) point out, there are numerous bodies that take reports of fraud and often the victim is unsure where to turn. This means that they may be known to many organisations, but each organisation may know about them only a few times; meaning that no one organisation will have a true picture of their victimisation and may therefore under assess their vulnerability.

2. Protection of Vulnerable Victims of fraud

After exploring the identification of victims, the questionnaire then went on to focus on how organisations protect their victims. As the responses came from the Police service some of the responses naturally covered the many initiatives in place to support victims, such as the Victims Code of Practice, already mentioned in earlier section of this dissertation. This code is for all victims, regardless of location or type of crime, and so was important to note in the responses seen, whether the respondents were dealing with 1,000 or 30,000 victims a month. A level of scrutiny must be brought to this promise however. To fully comply to these rules would require a comprehensive set of resources. It has already been noted by the HMICFRS (2019a) that many victims are suffering due to the downfalls of the central reporting system (NFIB) and the resulting delays due to volume of reports. Specific research into the different areas the code covers, and subsequent compliance levels, would be required to clarify this position.

When looking at vulnerability and repeat victimisation there is almost a ‘chicken and egg’ scenario. People can be classed as vulnerable due to them being repeatedly targeted, and those who are vulnerable can be repeatedly targeted due to the ‘success’ achieved by the offender in the past. There is therefore a need to protect those who are deemed vulnerable as there is an acceptance that many victims of fraud are targeted due to being vulnerable (Button et al 2014).

Questions were posed to try and obtain a key list of measures that organisations could put in place to prevent victims becoming victimised. The first key measure that runs through all of the responses is education. It is widely recognised that the volume of fraud offences means that it will never be tackled through investigation and so prevention work is key. This is emphasised by the fact that 80% of fraud and cybercrime is actually preventable and so time and resources should rightly be focused in prevention (City of London 2017). However, this does go against research conducted by Button et al (2009), where victims placed little emphasis on education, and more on getting their money back. In fact, many victims will not report what occurred to them if they have received their money back, or not actually incurred any loss (Button et al 2009a). This may include victims of identity theft for example, where their details have been stolen and attempts made to open accounts in their name have failed, or they have simply had the cards or loans cancelled due to them being fraudulent. This under reporting not only poses a problem for investigators, but victims also. First of all, if victims do not report then how can organisations assess their vulnerability? They may be highly vulnerable to further victimisation, for example they may lack the cognitive ability to identify a scam and sign up and share personal details again without thinking. The cycle of victimisation will therefore continue without the victim being highlighted for support and several chances are missed in educating the victim. The process is also bad for the victim as they may not truly learn from the mistakes they have made, or even worse, they may feel empowered to continue their risky behaviour, safe in the knowledge that they will be reimbursed any losses or that they won’t suffer losses in the future. This confidence will then cause them not to listen to concerns raised by those trying to offer crime prevention advice, rendering such efforts by investigators ineffective. This highlights the importance of proactive work being carried out by investigators to identify such victims at the earliest opportunity before this cycle has been commenced. If banks continually shut down fraudulently opened accounts and reimburse victims their lost money without sharing such information with other agencies, then they are the only organisation aware of the victim. No one would deny a victim compensation, but if this is provided with a support plan to share information with other relevant agencies to continue their education then surely this would be far more effective in the long run. Offenders are placed on a rehabilitation programme to support over several months, or years, to avoid re-offending. Whilst not as extreme as this, victims may also benefit from a continuous and monitored support scheme (Wedlock & Tapley 2016).

There is no doubt that victims today would still want to get their money back, most likely over a successful prosecution, but perhaps this is more reflective of current trends. The last ten years have seen some key changes; a huge increase in offences committed, technological advancements making it easier to commit and avoid detection, global movement of stolen property and a reduction in Police budgets. This means that education is the most cost-effective way of combatting fraud, not tackling the offenders directly but giving people the knowledge to protect themselves and disrupting offenders that way.

As part of this education it was discovered that the two most common ways it was provided was through the traditional means of face to face contact and relevant literature. Forces send out various types of literature, from general crime prevention advice to the 'Little Book of Big Scams' (LBOBS). The LBOBS is a book covering fraud prevention advice on all of the common fraud types, linking the reader to useful websites and giving them handy tips. Another respondent sent links to their website where all relevant advice was kept.

Whilst education is key, these results suggest that these measures were provided as a response to victimisation, responding to an event that has already happened and trying to prevent a repeat. As discussed previously, there needs to be an element of being pro-active and providing a message before victimisation has taken place. It is therefore pleasing to see that one respondent also visits communities and provides talks, potentially in a pro-active tactic. Clearly budgets will have an effect on how much expenditure can be afforded a pro-active crime prevention, with the added problems regarding measuring success to ensure effective use of resources, but in the age of digital media it is becoming easier to share messages to mass audiences instantly and cheaply.

HMICFRS (2019a) have recently been critical of forces for not being aware of the national fraud prevention campaigns that are supported and funded by Government and the financial sector. None of the respondents in this research referred to the national campaign of ‘Take Five’ or ‘Get Safe Online’. Whilst it is good for local officers to develop their own ways of communicating the message to their communities, the importance of a unified national campaign must not be overlooked. If the Government is trying to push out key messages but local forces are pushing out others, it may lead to confusion amongst the public as to who follow and what to believe.

This leads nicely on to the discussion of the internet and vulnerable victims of fraud. Is providing advice on the internet and through social media and effective way of targeting vulnerable victims? More people than ever are now using the internet but there are still many elderly people who do not use the internet, or truly understand how it works. This means that online advice may only be targeting a limited amount of people. Many forces may become complacent in using social media and simply expect everyone will come to them and read the message, rather than reaching out and spreading it to those who wouldn’t normally hear it but would fall victim to fraud.

One way of reaching these people is through working with other partners. Two of the respondent’s use a multiagency approach to protect vulnerable victims, linking in with the CECAS (Cyber & Economic Crime Awareness Service). One such example comes in Manchester where after multiple sources of data are used to identify vulnerable victims, victims are then signposted to other support services and partner agencies. This multi-agency approach has been adopted in many areas of policing and been seen to improve services (Shearlock & Cambridge 2009) so it should be no different in this area either. This also emphasises that support will be a continued process, not simply a one-off after reporting an incident. This will help reinforce messages with victims and keep a line of communication when they may be susceptible to further contact from offenders. It is well known that fraudsters have excellent 'powers of persuasion' and their skills lie in convincing people of the lie that they are selling. It is also known that previous victims details are passed or sold between offenders, often referred to as 'suckers lists' (Murray 2018). Victims of investment scams are quite commonly re-contacted with offers to recover their investments for a small fee (Get Safe Online 2019) or romance scam victims may still receive communication from the offender who tries to convince them they are legitimate. This repeat contact allows any follow up calls from the offenders to be challenged and the victim to be reminded of their advice.

Evidence has shown that this is one of the best ways to support victims, helping prevent further victimisation and keeping them engaged with the criminal justice system (Wedlock & Tapley 2016). Due to the reforms of the Victims Code in 2013 and 2015, the government have developed national policies on improving victims' services and the value that support services bring to the criminal justice system is now widely acknowledged (Wedlock & Tapley 2016). These services take the burden from the police and provide a boundary for victims between the prosecution of offenders and support of victims. There are numerous models in which this multiagency work can be approached, covering not only information sharing but also a coordinated intervention in a Multi-agency Safeguarding Hub (Home Office 2014).

Organisations must not become dependent on such systems though as they will only work if all the agencies involved are committed to performing as they have agreed (Home Office 2014). Often organisations like to adopt the latest ways of working without truly understanding what they mean and ensuring they are regularly reviewed to ensure they are working. If organisations share relevant information they have to ensure there is someone who will take responsibility and assist the victim. They also need to have the confidence to share information, with one of the main criticisms being that organisations still frequently hold information back which could be of assistance to others (Home Office 2014).

Another key area that was raised revolves around training staff members. By training as many people as possible in this area an organisation will increase its chances of identifying vulnerability as each and every time that victim has contact with a member of their organisation they will be reviewed accordingly. This spreads the burden, and risk, of leaving it to frontline workers, or specialist departments missing a case due to the volume of cases to review.

As discussed, much work is being done on the prevention side of policing with specialist posts being created to raise awareness of fraud and trying to educate potential future victims. One respondent however points to the proactive targeting of offenders. They prioritise investigations against those most vulnerable but also look at disrupting the offenders causing most harm to the community. Whilst victim services are vital in supporting those that have become victims, it raises the valid point that if the offenders of such crimes are brought to justice and are pro-actively targeted then there will ultimately be less victims to support. The positivity around offenders being brought to justice may also provide solace to victims in knowing that action is being taken against the type of people who targeted them. It would therefore be remiss of any force not to consider a pro-active disruption approach to protecting future victimisation, nor to forget the power of bringing offenders to justice when supporting victims.

3. Areas for Improvement in the sharing of data

It has already been established that respondents to this questionnaire, and police forces on the whole, share information with partner agencies for the prevention and detection of crime. This section was primarily aimed at the private sector to gain a greater understanding of their processes. Although there are no results from this sector it was still important to review the Police's sharing protocols and identify any areas for improvement.

As discussed, it was confirmed that police forces share data on victims with relevant safeguarding teams and some limited other organisations including Age UK and banks. This data sharing allows organisations working towards similar goals. i.e. protecting the public, improve this fight and has been seen in many areas of policing already, such as domestic violence for example. Initiatives such as the 'Banking Protocol' – stopping around £38 million of fraud in 2018 alone – shows how powerful this collaboration can be (UK Finance 2019). The Police have always needed the publics support in protecting others in society and through sharing crime prevention advice and training they have created a safe data sharing environment that prevents losses to the banks, prevents losses to the victims and improves the fight against crime.

Respondents have indicated that data is shared on an ad hoc basis and can be in writing or verbal as per the requirements of the incident. They are also very keen to share data to improve their own, and other organisations abilities, to protect the vulnerable.

Feedback received from the questionnaire indicated that organisations would like an agreed protocol for sharing with clear pathways on what form is required and where it is to be sent to. It is believed that this standardisation between organisations would ensure that each party were clear on what they were asking for and what they required back. It would also help direct the request to the relevant person who could share it, rather than a mixture of requests coming in to different people within the organisation. These same principles would also apply for when organisations would want to push out intelligence to others, not simply for the process of requesting information. Some concerns were raised about other organisations not acting on information as quickly as the respondent would have wanted. Again, through setting up clear agreements it should avoid this frustration.

The recording and justification of such requests was highlighted as a key area. A standard form would not only help avoid any ambiguities in what was being asked for, but also clearly record under what legislation it was being requested or shared under. This would allow a transparent overview of what was being undertaken and simplify any reviews of the process to ensure compliance. It would also help protect those sharing it should any legal challenges be brought. These forms could also be given the flexibility of being completed post event, to allow for exceptional circumstance where the information needed to be shared immediately, for example under the ‘Banking Protocol’. This would maintain the relevant records but not hinder the process when operational demands required it.

Multiple pieces of legislation allow for the sharing of data for protecting vulnerable people. Perhaps this is an issue regarding awareness amongst officers, or perhaps a key insertion into the Data Protection Act is required. It is clear that one respondent wants to share data but is concerned about how to do so legally. It would be a great shame for there to be multiple ways of sharing data, legally, which weren't known and thus hindered the sharing of the information. We appear to live in a culture where everyone is reluctant to talk to others for fear of breaching data protection acts. Very often there is a genuine, legitimate reason for sharing information that will benefit organisations in protecting victims. In these situations the law has (usually) made allowances for this. Investigators who do not know of such allowances will then be hampered in effectively supporting victims. Similar concerns were expressed though later in the research when talking about barriers to share information as one respondent found other organisations compliance teams to be very risk adverse and reluctant to share information. Again, it may require more simplistic legislation to ensure confidence is fostered by the relevant people to allow the sharing of such data, or simply shows the learning need is far more reaching than first thought.

Once this understanding has been gained it is clear from the responses in the research that there is a wealth of information Police forces could share. This includes methodologies around victim care, crime prevention advice and the latest scam trends that have been identified. Sharing knowledge on how different organisations deal with vulnerable victims of fraud is a fantastic way of improving the service given to victims. Sharing the mistakes, sharing what works well, all goes towards providing society with a better service. This appears to be happening with CIFAS collating a national fraud database to help organisations from different sectors share intelligence (CIFAS 2019a). The issue of sharing the latest scams and crime trends is also a very worthwhile practice. Those organisations taking calls from victims are seeing the trends live. As fraud is often a borderless crime (Button 2012), both nationally and internationally, it can be hard to keep up-to-date with the ever changing landscape.

The National Fraud Intelligence Bureau uses all the reports made through to Action Fraud to analyse trends and share them with partner agencies. Questions must be raised however over the speed of this analysis when thousands of reports are received each month and so there is ultimately likely to be a back log of reviews.

Whilst there was clearly much positivity around the sharing of information, naturally there were some concerns regarding the overall benefits of doing so. One respondent felt that sharing data in individual circumstance would be of benefit to protecting that victim, but sharing data on mass may not be as beneficial. As referred to many times before, the sheer volume of fraud and victims may mean that if data is shared 'en-mass' then key victims are missed and it becomes a generic data washing exercise. Another respondent raised the fact that despite their efforts to share the relevant information with other agencies, to educate the public and share information with them, they still continually see the high volume of victims they have always seen. They even point out the fact that they use the same lines of communication that fraudsters do, i.e. they warn people online about the danger of online scams. This therefore raises questions around the success of the methods being currently employed and the value in sharing the information organisations currently are. When looking at initiatives such as the 'Banking Protocol' and the amount of money that has prevented from entering criminal pockets there can be no question of the value of this work. The 'Banking Protocol'' relies on real time information with a rapid response from the Police. Could timeliness of information sharing be hindering the overall prevention work? Are organisations sharing the right data but not quick enough? Are they actually sharing the right information? Does fraud hit upon a cultural issue in that due to the 'on-demand' society we live in we expect everything now, we trust technology, we want that bargain and accept that everyone so often we will be caught out? Do we accept that in order to live in a digital, fast pace world, that at some point our security will be compromised?

Although the questions appear to have been misinterpreted in this research, the topic of how often and in what format organisations would like to receive information was covered. Would organisations like a live update of vulnerable victims or a monthly list for example? In terms of use, could they cross reference the victim list with their own databases to identify previously unvisited victims? Would banks like to receive a list of vulnerable victims from trading standards or police so they could put extra alerts on certain customers to protect them? In knowing how organisations might use the information it would help tailor the information shared. If the information was not going to be processed by others then it would be a waste of time for all involved sharing it. Unfortunately, due to the level of responses these questions remain unanswered.

Due to most frauds requiring a banking element at some point it was hoped banks would participate in the research and so a greater understanding of their practices could be gained. It is difficult to know how much information banks share with each other. With the new 'Open Banking' regime taking shape it may be that they will soon share more information than ever before (Peachey 2018), but as fierce competitors there is still likely to be a lot of banking organisations reluctant to share information. There is a well-established scheme of reporting 'Suspicious Activity Reports (SARs)' that the National Crime Agency oversee (NCA 2019a). This is clearly a way that banks share information with other regulated organisations and so may be a way they share information on victims. How responsive, or how comprehensive this is when it comes to the identification and protection of vulnerable victims is unknown. A recent publication highlights that the National Crime Agency have a specialist unit set up to review the incoming SARs to highlight any vulnerable victims and ensure they fast tracked and passed to local law enforcement (NCA 2019b).

Stepping aside from the debate around the positives and negatives for sharing such information, the research sought to identify potential barriers from such a scheme even starting. One of the first barriers is certainly a key one; the victim's reluctance to share their information with other organisations or report their crime in the first place. As Button et al (2009) states, many people will blame themselves for falling victim to a fraud and therefore won't report it due to the embarrassment. If they do decide to report it then they will scrutinise any unsolicited call or communication to a far higher level than before. Quite understandably, a victim of identity theft is unlikely to want to share their details with several organisations for future advice as they will be overprotective of their personal information. Research conducted by Button et al (2014) found that one victim of ID theft changed his behaviour so much that he regularly refuses to reveal his real name and goes to other great lengths to conceal his identity. This means that although it would be useful for organisation to share such information with other agencies to offer a greater level of victim support, they are unable to do so because they don't have the victim's consent. This would be an unavoidable barrier to share such data.

In certain circumstances though data sharing would be possible without the victim's consent. The banks do have the option of disclosing the information if it is the public interest to do so, under the 'Tournier Rules' as set out in 'Tournier v National Provincial and Union Bank of England 1924 (Abdulah 2013). This may occur where they see a customer who appears to be a being financially abused and is likely to be only used in exceptional circumstances.

A final question was posed to the respondents asking if they had anything else relevant they felt they wanted to add. One respondent raised their concerns again about reaching those victims who don't engage with reporting crime and don't engage with media campaigns to prevent their victimisation. It could be argued that these are the truly vulnerable victims of crime as they being targeted and falling victim to crime, but are out of reach or not engaging with support services and the relevant authorities. There are campaigns trying to address this area, such as the #Tell2 campaign from the City of London Police whereby everyone is encouraged to tell two people who aren't online about the relevant fraud prevention message (Twitter 2018) It is a very difficult area to solve, but one that must be considered and included in any prevention strategy when organisations are trying to protect victims.

The final points focused on ensuring the Police were getting the right balance between focusing on victims and focusing on offenders, and using the full intelligence picture to its full potential. Every investigator has to balance the needs of the investigation with the needs of the victim. This answer raises an interesting debate; in placing all our attention on the victim are we losing sight of tackling the offenders? There will always be merit in supporting victims, but if offenders are tackled successfully then investigators may stop innocent people falling victim to fraud. Is it better to focus on this area and prevent as many crimes as possible, or provide better support to those who have fell victim? The obvious answers would be to perform both functions or reach a balance. This all depends on how resources are funded and prioritised though. If organisations develop their 'protect' officers and reduce budgets of investigators, then they are naturally gearing themselves up to lean towards protect services over pursuit of offenders. Could investigators perform their investigative duties and partnership agencies undertake the supporting of victims and assisting in prevention strategies?

This way each organisation sticks to its core skills and functions, working close enough to allow for continuous feedback?

CONCLUSION

It is clear that unfortunately due to the low response rate the research has received that true conclusions may not be drawn from the research. However, that is not to say that there aren't some key messages and learning points that organisations can draw from it. As the responses came from Police forces then any conclusions may be more relevant for public sector organisations, but there are certainly relevant points that the private sector can take into their working.

In terms of identifying vulnerability the police face a difficult task. The centralised system of reporting fraud takes the initial review out of forces hands, instead relying on other call takers to identify vulnerability, or even more despairingly victims providing enough information to the online reporting system to highlight themselves as vulnerable. Despite this, forces show a strong desire to identify vulnerability amongst fraud victims, employing wide ranging definitions to not preclude victims from falling into the cope of vulnerability, whilst providing key words and specific characteristics to ensure all those who assess vulnerability have a solid framework to work from. This negates issues with inexperienced assessors and does not prohibit 'common sense' or professional judgement. Although those on the front line should be afforded the opportunity to develop their practices through experience and tailor them to their force's needs, through wider literature this appears to create inconsistency amongst victim support and a 'post code lottery'. There needs to be greater communication on what works, fed back into the central lead force City of London Police to ensure a greater consistency for victims. Although the HMICFRS have compiled numerous reports and provide forces with guidelines on best practice this is not always being followed. Whether the forces have improved on the recommendations in place is for further research to establish, but it is clear that forces should be bringing these improvements to the attention of the HMICFRS to improve the overall protection of victims.

One issue that was touched upon by a respondent was that someone’s vulnerability can be affected by their “mental, physical or social circumstances”. How deeply they interpret this is unclear, but it was the only comment that appears to reflect on vulnerability as being a fluid process. The definitions of vulnerability given by the respondents were broad and open ended to allow a wide range of victims to be included, but there appears to be a lack of consideration in the assessment process on how individuals may easily flow in and out of a vulnerable state. For example, a person who has just lost a partner may be more susceptible to a romance scam as their emotions run high and they look to fill the loneliness they feel. Overtime however as they settle, they might regain control of their emotions and recognise a scam for what it is. Likewise, an investor may not be a vulnerable person, but as the scam unfolds and they realise that they are facing a huge financial loss they may become vulnerable to further victimisation as they are offender the chance to recover money by another fraudulent group, investing further and spiralling out of control as they chase their money back. Organisations making such vulnerability assessments need to be aware of these changing factors and although they can’t be expected to constantly re-assess victims, an understanding of this issue is vital to provide the best service.

After the protection of life, one of the key priorities for the Police is to keep law and order and bring offenders to justice. This may naturally affect their response to vulnerable victims of fraud and mean that they focus on a witnesses ability to provide evidence, rather than an overall service including support. Especially with the evertightening budgets imposed on them, their resources are being stretched as thinly as ever and so they may only be able to meet the minimum standard of victim care as set out in legislation, when many victims would require further support. This will be one of the driving forces in seeking support from other organisations, and the voluntary sector, in providing this further care, e.g. the CECAS. This means that partnership working is vital for victims, although forces must ensure that safeguards and continuous evaluation systems are in place to ensure that those organisations they are out-sourcing responsibilities to are fit for purpose. It may also question whether all victim care services should be outsourced, allowing the Police to focus on their primary functions, supporting victims through bringing them justice and preventing further victimisation by disrupting offenders. With over two thirds of cases not being investigated and victims requiring continual support due to the nature of fraud victimisation, would this rebalancing of responsibilities provide the public with a better service? Has the emphasis on identifying and protecting victims detracted from the benefits of pursuing offenders, disrupting their activities and bringing them to justice?

What is also clear from the research is that education plays a large part in the Police's response to protecting victims, a fact that is probably not surprising when considering how much fraud is actually preventable. Whilst not denying the importance of such education, further research into the effectiveness of such education would be highly valuable to practitioners, a point raised by one respondent. Should the education be targeted at the younger generation? Or the older generation? In what format? How should it be delivered? Online or offline? What about those who don't want to be educated? There will still be victims out there who don't report because they don't realise they have become victims, or they don't want to believe they have. How can they be educated? Victims of romance scams often hold onto the belief that they are in a relationship, that they are not a victim, or investment fraud victims believe their investment will mature, or they weren’t defrauded but actually chose a bad investment. These coping mechanisms and strategies can be so ingrained in victims that they can’t see past it. It may be that organisations have to accept that there will be a certain number of victims who can’t be protected, and they will never prevent further victimisation in some cases.

The low response rate to this research can be shown as indicative of the culture currently seen around the sharing of data. It is clear practitioners want to share data to protect victims but face barriers to doing so. These barriers do not necessarily come in terms of legislation, but the confidence and knowledge in the mechanisms in which they can be shared. Suggestions to tackle this came around the creation of specific pieces of legislation that clearly state that the sharing of data is permitted to protect vulnerable victims. It could be argued that this isn’t actually required when safeguards are in place already and in fact education is all that is needed, but if the process was simplified and it gave practitioners confidence then perhaps it would achieve its purpose.

Questions have been raised though that even if this sharing of data was made simple, clear and easy to complete, would it actually benefit the process of protecting victims? It is clear from other literature that this sharing of data can work but only if all those who want to share it will support and take responsibility for acting upon it, and openly share what they have. The current networks the Police share data through are mainly centred around other public sector bodies. Perhaps these may not provide the overall effect desired in terms of protecting victims. This is where the research tried to develop ideas for public - private sector collaboration as it is felt this is where real value may lie in data sharing, as seen in success through the ‘Banking Protocol’.

Despite recent inspections and improvements in the landscape of fraud in the Police, even from the small sample size in this research, it is widely accepted that there appears to be a disjointed response amongst forces (HMICFRS 2019a). It is perhaps fair to argue therefore that before collaborative work is considered outside of the public sector, that the public sector is 'singing from the same hymn sheet' and have developed a common and consistent approach. Otherwise the private sector will face mixed responses when communicating with different forces and struggle to effectively work with them. Ironically, the research conducted highlighted the request for a clearly defined pathway and protocol for sharing information, showing the need for uniformity to allow confidence in the process.

A key issue in this area, and no doubt most in policing, is funding. It is recognised that this is impactive on the resources ultimately put into protecting victims (HMICFRS 2019a). Whilst a key issue, it would be easy to blame this for any failings and lack of improvement. This research highlights that there are some new collaborative projects ongoing, such as the CECAS, and so there are ways to overcome the issues of funding. It would appear the greatest value could come through the evaluation and sharing of these ways to allow other forces to enjoy the benefits.

The success of any new procedure put in place will always be hampered by the inability to accurately measure its success. This is because the true nature and scale of fraud is not understood or recorded, making the already difficult task of measuring prevention work even harder.

However, it is clear that investigators want to protect vulnerable victims, they are doing so, and, they are trying to innovate and seek new ways to improve their fight. Part of this fight needs to include collaborative working, which is essential for victims to be able to get the support they require (Tapley 2016).

APPENDIX

Appendix A

- UK Police Forces
    - Metropolitan
    - West Midlands
    - Greater Manchester
    - West Yorkshire
    - Thames Valley
    - Merseyside
    - Kent
    - Northumbria
    - British Transport
    - Devon & Cornwall
    - City of London
    - Warwickshire
    - Wiltshire
    - Gloucestershire
    - Suffolk
    - Lincolnshire
    - Cumbria
    - Bedfordshire
    - Durham
    - Gwent

- Banks
    - Lloyds
    - Royal Bank of Scotland
    - Halifax
    - HSBC
    - TSB
    - NatWest
    - Halifax
    - Barclays

    - Nationwide
    - Santander
    - Metro Bank
    - Standard Chartered
    - Co-operative Bank
    - Sainsburys Bank
    - Tesco Bank
    - Virgin Money
    - Yorkshire Bank
    - Western Union
    - MoneyGram
    - Monzo
    - Atom
    - Fidor
    - Revolut
    - Starling
    - Tandem
    - APS Financial

- Serious Fraud Office
- National Trading Standards
- Financial Conduct Authority
- Capita (British Gas)
- EON
- Charities Commission
- Insolvency Service
- HMRC
- Gambling Commission
    - Gambling Companies
    - Bet365
    - Ladbrokes
    - Royal Panda
    - Betfred
    - Paddy Power
    - 888 Sport

    - Betfair
    - Bet Victor
    - Coral
    - William Hill

- Insurance Fraud
    - Aviva
    - AXA
    - Admiral
    - Direct Line
    - Liverpool Victoria
    - Hastings
    - Churchill

Appendix B

1. Which sector you are employed in? E.g. Police, Banking, Insurance

1.a. What is your job title?

2. How does your organisation define vulnerability?

3. What characteristics or criteria does your organisation use to define vulnerability?

4. How does your organisation identify vulnerability?

5. What sort of processes does your organisation follow to make such identification?

6. How did your organisation decide on these factors?

7. What data sources does your organisation use to identify vulnerability?

8. What methods does your organisation employ to protect vulnerable victims?

9. What measures does your organisation take to try and prevent repeat victimisation?

10. What fraud prevention advice does your organisation provide?

11. How many vulnerable victims does your organisation identify each year?

12. What resources does your organisation have available to support victims?

13. How does your organisation prioritise victims?

14. Does your organisation currently share data with other agencies to help the protection of vulnerable victims?

14.a. If so, What type of information does your organisation share?

14.b. With whom?

14.c. How is the data shared?

14.d. How could these processes be improved?

15. Do you think organisations should share data to protect vulnerable victims?

16. How do you think this should be done?

17. What information would your organisation like to receive?

17.a. How often?

17.b. How would your organisation use it?

18. What information could your organisation share to potentially assist others?

18.a. Do you think this would benefit the overall protection of vulnerable victims?

18.b. What barriers do you see preventing the sharing of this information?

19. If you have any other comments in relation to the topic matters discussed above please feel free to add them here

Appendix C

18/08/2019 University of Portsmouth Myport Mail - Re: Ethics Submission for MSc

Matthew John Newell <up878163@myport.ac.uk>

Re: Ethics Submission for MSc

1 message

icjsethics - <icjsethics@port.ac.uk> 2 May 2019 at 16:36 To: Matthew.Newell1@myport.ac.uk, Jacki Tapley <jacki.tapley@port.ac.uk>

Dear Matthew,

Thank you for re-submitting your ethics documentation. We have reviewed this submission and are providing a provisional favourable ethical opinion with the following requirements:

1. The title of your study should be consistent throughout, from the title of your ethics form onward.
2. Please be consistent about the potential for withdrawal from the study, this is **not** possible once

the survey has been submitted.

3. Please confirm that your contacts in the different organisations will act as gatekeepers and disseminate your survey. It is very important that the potential participants do not feel compelled to participate, so all invitations to take part must go through a gatekeeper with the invitation letter.

4. The consent form is embedded in your online survey, so they will not need to send you separate copies of the consent form, as you suggest in the invitation letter – please amend this.

5. Please note, and change in your information sheet section, that the current Chair of the ICJS Ethics Committee is David Shepherd (david.shepherd@port.ac.uk).

Your supervisor will be responsible for ensuring that these requirements have been met before any data collection can take place.

Please note your ethics reference number is 356. Good luck with your research,
Regards
Andie

11. Declaration by Principal Investigator and Supervisor

1. The information in this form is accurate to the best of our knowledge and belief and we take full responsibility for it.
2. We undertake to conduct the research in compliance with the University of Portsmouth Ethics Policy, UK Concordat to Support Research Integrity, the UKRIO code of Practice and any other guidance we have referred to in this application. University of Portsmouth Research Data Management Policy. ‘
3. If the research is given a favourable opinion we undertake to adhere to the study protocol, the terms of the full application as approved and any conditions set out by the Ethics Committee in giving its favourable opinion.
4. We undertake to notify the Ethics Committee of substantial amendments to the protocol or the terms of the approved application, and to seek a favourable opinion before implementing the amendment.
7. We are aware of our responsibility to be up to date and comply with the requirements of the law and relevant guidelines relating to security and confidentiality of personal data, including the need to register, when necessary, with the appropriate Data Protection Officer. WE understand that we are not permitted to disclose data identifying individuals to third parties unless the disclosure has the consent of the data subject.
9. We understand that research records/data may be subject to inspection by internal and external bodies for audit purposes.
11. I understand that the information contained in this application, any supporting documentation and all correspondence with the Ethics Committee and its Administrator relating to the application:

- Will be held by the Ethics Committee until at least 3 years after the end of the study’
- Will be subject to the provisions of the Freedom of Information Acts and may be disclosed in response to requests made under the Acts except where statutory exemptions apply.
- May be sent by email or other electronic distribution to Ethics Committee members.
- Will be subject to the provisions of the ‘DPA 1998’

Student name and number Matthew NEWELL (878163)
Date 18.04.19
Signature M. NEWELL
Supervisor Dr Jacki Tapley
Date 03.04.19

Signature ……… …………….

To whom should I send my completed application?
A single document, incorporating all essential elements, should be sent to the ICJS Ethics Committee at icjsethics@port.ac.uk.
How long will the review take?
Ethical review is normally undertaken within a period of 10 working days but you should allow a day or two at each end of this period for necessary administration. Ethics committees may also require a response and then need to review your response, again normally within 10 working days. This is why it is safest to allow three weeks for your application to be approved.
Date complete ethical bundle received fit for review: …29.4.19………………………………………

Date reviewed: ......2.5.19................……………………..

Signed: ....Dr Andie Shawyer...…............... (Member of ICJS Ethics Committee)

What sort of response can I expect from the Committee?
PLEASE DO NOT DELETE THE PART BELOW

ICJS EC Ethical Opinion Outcome Record*	
Favourable ethical opinion **You can commence data collection with the agreement of your supervisor.**	
Provisional favourable ethical opinion subject to requirements. **See ‘Comments’ on following page.** **Once your supervisor is satisfied that you have met these requirements, you may commence data collection.**	**X**
RISKS ASSESSED AS SIGNIFICANT and a favourable ethical opinion cannot be provided for the proposal in its present form. **See ‘Comments’ on following page.** **You must revise your proposal in consultation with your supervisor. Once your supervisor is satisfied that you have addressed all of the Comments below, you may resubmit for ethical opinion** **You may not commence data collection.**	

YOU MUST NOT ATTEMPT TO COLLECT ANY DATA NOT ALREADY PUBLICLY AVAILABLE UNTIL A FAVOURABLE OPINION HAS BEEN ISSUED

Comments:

Thank you for re-submitting your ethics documentation. We have reviewed this submission and are providing a provisional favourable ethical opinion with the following requirements:

1. The title of your study should be consistent throughout, from the title of your ethics form onward.
2. Please be consistent about the potential for withdrawal from the study, this is **not** possible once the survey has been submitted.
3. Please confirm that your contacts in the different organisations will act as gatekeepers and disseminate your survey. It is very important that the potential participants do not feel compelled to participate, so all invitations to take part must go through a gatekeeper with the invitation letter.
4. The consent form is embedded in your online survey, so they will not need to send you separate copies of the consent form, as you suggest in the invitation letter – please amend this.
5. Please note, and change in your information sheet section, that the current Chair of the ICJS Ethics Committee is David Shepherd (david.shepherd@port.ac.uk).

Your supervisor will be responsible for ensuring that these requirements have been met before any data collection can take place.

REFERENCES

Abdulah, S (2013). *The Bank's Duty of Confidentiality, Disclosure Versus Credit Reference Agencies; Further Steps for Consumer Protection*: *'Approval Model'.* Eurpoean Journal of Current Legal Issues, Vol 19, No 4. Available online at http://webjcli.org/article/view/296/405#_edn9

Action Fraud (2019). *A-Z Fraud*. Actionfraud.police.uk. Available online at https://www.actionfraud.police.uk/a-z-of-fraud-category/other

AGE UK (2015). *Only the tip of the iceberg: Fraud against older people, evidence review*. Available online at https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

BBC (2018). *'Romance fraud': Online dater, 86, conned by woman*. BBC.com. Article dated 29th June 2018. Available online at https://www.bbc.co.uk/news/uk-england-derbyshire-44657349

Blakeborough, L. & Correia, S.G. (2018). *The scale and nature of fraud: A review of the evidence.* Home Office review. Retrieved from the UK Home Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf

Button, M. , Johnston, L. , & Frimpong, K. (2008). *The Fraud Review and the policing of fraud: laying the foundations for a centralized fraud police or counter fraud executive?* Policing, 2(2), Pages 241-250. https://doi.org/10.1093/police/pan027

Button, M. ,Lewis, C. & Tapley, J. (2009). *Fraud typologies and the victims of fraud: literature review.* London: National Fraud Authority. Available at http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-typologies-and-victims.pdf

Button, M. , Lewis, C. & Tapley, J. (2009a). *Support for the Victims of Fraud: An Assessment of the current Infra-Structure in England and Wales*. London: National Fraud Authority. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118470/support-for-victims-of-fraud.pdf

Mark Button, (2012). *Cross-border fraud and the case for an "Interfraud"*. Policing: An International Journal of Police Strategies & Management, Vol. 35 Issue: 2, pp.285-303, https://doi.org/10.1108/13639511211230057

Button, M. , Lewis, C. , & Tapley, J. (2014). Not a victimless crime: the impact of fraud on individual victims and their families. Security Journal, 27(1), 36-54. https://doi.org/10.1057/sj.2012.11

CIFAS (2019). *30 facts about fraud, past, present and future.* Available online at https://www.cifas.org.uk/insight/30-facts-about-fraud-past-present-future

CIFAS (2019a). *National Fraud Database*. Available online at https://www.cifas.org.uk/services/national-fraud-database

City of London (2017). *National Policing Lead For Economic Crime Annual Review 2016 – 2017*. Available online at https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Documents/ecd-annual-review-201617.pdf

Cross, C. (2016). *Why we need to do more for the victims of online fraud and scams*. Published 19th May 2016. Available online at http://theconversation.com/why-we-need-to-do-more-for-the-victims-of-online-fraud-and-scams-59670

CPS (2019). *Special Measures*. CPS.gov.uk. Last update July 2019. Available online at https://www.cps.gov.uk/legal-guidance/special-measures

Davies, P. , Francis, P. & Greer, C. (2017). *'Victims, Crime and Society: An Introduction' (2nd Ed)* London: Sage. Second edition.

Drew, M. & Farrell, L. (2018). *Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs*. Police Practice and Research, An International Journal. Published by Routledge, Taylor & Francis Group and available at DOI https://doi.org/10.1080/15614263.2018.1507890

Evans, M. (2017). *Fraud and cyber-crime are now the country's most common offences.* Telegraph.co.uk. Article dated 19th January 2017. Available online at https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/

FT.com (Financial Times) (2018). *UK's new economic crime fighting centre set to open*. Article dated 3rd September 2018. Available online at https://www.ft.com/content/82aa848e-af7b-11e8-8d14-6f049d06439c

Gartside, S. (2018). Online-only banks – six digital-only banks. Article dated 16th March 2018. Available online at https://www.savvywoman.co.uk/2018/03/online-only-banks-six-digital-banks/

Get Safe Online (2019). *Recovery Room Scams.* Available online at https://www.getsafeonline.org/protecting-yourself/recovery-room-scams/

Greer, C. (2017). 'News Media, Victims and Crime' in P. Davies, P. Francis and C.Greer (2017) (2nd Ed) *Victims, Crime and Society. An Introduction*. London : Sage.

Greaves, E. (2018). *Don't blame consumers for fraud and scams, banks warned*. Moneywise.co.uk. Article dated 22nd August 2018. Available online at https://www.moneywise.co.uk/news/2018-08-22/dont-blame-consumers-fraud-and-scams-banks-warned

Grierson, J. (2016). *Met chief suggests banks should not refund online fraud victims*. Article dated the 24th March 2016. Available online at https://www.theguardian.com/uk-news/2016/mar/24/dont-refund-online-victims-met-chief-tells-banks

Hamlyn, B. , Phelps, A. , Turtle, J. & Sattar, G. (2004). *Are special measures working? Evidence from surveys of vulnerable and intimidated witnesses*. Home Office Research Study 283. Home Office Research, Development and Statistics Directorate June 2004. Retrieved from the College of Policing website: http://library.college.police.uk/docs/hors/hors283.pdf

Home Office (2014). *Multi Agency Working and Information Sharing Project Final report*. Published July 2014. Available online at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/338875/MASH.pdf

Home Office (2016). *Home Secretary launches new joint fraud taskforce*. Published on 10th February 2016 and available online at https://www.gov.uk/government/news/home-secretary-launches-new-joint-fraud-taskforce

HM Government (2018). *Victims Strategy*. Published September 2018 and retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746930/victim-strategy.pdf

HMICFRS (2018). *PEEL: Police effectiveness 2016, A vulnerability revisit inspection of Hertfordshire Constabulary.* Published March 2018 and available online at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/hertfordshire-peel-vulnerability-revisit-2016.pdf

HMICFRS (2019). *PEEL spotlight report, A system under pressure*. Published 2019 and available online at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-spotlight-report-a-system-under-pressure.pdf

HMICFRS (2019a). *Fraud: Time to Choose, An inspection of the police response to fraud*. Published April 2019 and available online at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf

HMICFRS (2019b). *The poo relation, The police and CPS response to crimes against older people.* Published July 2019 and available online at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/crimes-against-older-people.pdf

London.gov (2018). *Economic Crime Victim Care Unit Grant for 2018-20*. Available online at https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/mopac-decisions-0/economic-crime-victim-care-unit-grant-2018-20

Macpherson, C. (2001). *The Youth Justice and Criminal Evidence Act 1999: Achieving Best Evidence?*. Medicine, Science and the Law, 41(3), 230–236. https://doi.org/10.1177/002580240104100305

McKim, A (2017). The Value of Mixed Methods Research: A Mixed Methods Study. Journal of Mixed Methods Research 2017, Vol. 11(2) 202–222. Published by Sage and available at DOI: 10.1177/1558689815607096.

Ministry of Justice (2012). *Post-legislative assessment of the Fraud Act 2006, Memorandum to the Justice Select Committee*. Published June 2012 and retrieved from https://www.justice.gov.uk/downloads/publications/corporate-reports/MoJ/2012/post-legislative-assessment-fraud-act-2006.pdf

Ministry of Justice (2015). *Code of Practice for Victims of Crime*. Published October 2015 and retrieved from https://consult.justice.gov.uk/digital-communications/victims-code/results/code-of-practice-for-victims-of-crime.pdf

Mythen & McGowan. (2007) 'Cultural victimology revisted' in S. Walklate (2007) Handbook of Victims and Victimology. Published by Willan Publishing.

Mothershaw, N. (2017). *Fraud still costing the UK more than £190bn – new analysis released in the Annual Fraud Indicator*. Experian.co.uk. Article dated 16th November 2017. Available online at https://www.experian.co.uk/blogs/latest-thinking/identity-and-fraud/fraud-costing-uk-more-than-190bn-released-annual-fraud-indicator/

Murray, A (2018). Sucker list: 'Fraudsters stole £280,000 from me in 2017 - and took £11,000 a year later'. Telegraph.co.uk. Artciel dated 31st March 2018. Available online at https://www.telegraph.co.uk/personal-banking/savings/sucker-list-fraudsters-stole-280000-2017-took-11000-year-later/

National Post (2017). *Desperate businessman commits suicide after losing $300K in investment scam: 'The house always wins'*. Nationalpost.com. Article dated 5th March 2017. Available online at https://nationalpost.com/news/canada/desperate-businessman-commits-suicide-after-losing-300k-in-investment-scam-the-house-always-wins

NCA (2019). *National Economic Crime Centre.* Nationalcrimeagency.gov.uk. Available online at https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre

NCA (2109a). *Suspicious Activity Reports.* Nationalcrimeagency.gov.uk. Available online at https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing/suspicious-activity-reports

NCA (2019b). *SARS In Action, Safeguarding the Vulnerable.* Nationalcrimeagency.co.uk. Available online at https://nationalcrimeagency.gov.uk/who-we-are/publications/268-ukfiu-sars-in-action-march-2019/file

Noaks, L., & Wincup, E. (2011). *Negotiating and Sustaining Access, Criminological Research* (pp. 54-73). Available at http://dx.doi.org/10.4135/9781849208789

O'Hara ,M. (2015). Why is our justice system failing vulnerable people?. Theguardian.com. Article dated 9th September 2015. Available online at https://www.theguardian.com/society/2015/sep/09/prison-system-failing-vulnerable-people

Peachey, K (2018). *Open Banking 'revolution' to challenge banks' dominance*. BBC.com. Article dated 12h January 2018. Available online at https://www.bbc.co.uk/news/business-42655716

Peachey, K (2019). *Women 'victims in 63% of romance scams'*. BBC.com. Article dated 10th February 2019. Available online at https://www.bbc.co.uk/news/business-47176539

Reisig, M.D. & Holtfreter, K. (2013). *Shopping fraud victimization among the elderly*. The Journal of Financial Crime, Vol. 20 Issue 3, pp 324 – 337. Published by Emerald Insight and available at https://doi.org/10.1108/JFC-03-2013-0014

Relbanks (2018). *Banks in the UK*. Available online at https://www.relbanks.com/europe/uk

Robbins, J. (2018). *Exclusive: more than 96% of reported fraud cases go unsolved*. Which.co.uk. Article dated 24th September 2019. Available online at https://www.which.co.uk/news/2018/09/exclusive-more-than-96-of-reported-fraud-cases-go-unsolved/

Rock, P. (2018). 'Theoretical perspectives on victimisation' in S. Walklate (2018) (2nd Ed) *Handbook of Victims and Victimology*. Published by Routledge.

Scheibe, S. , Notthoff, N. , Menkin, J. & Ross, L. (2014). *Forewarning Reduces Fraud Susceptibility in Vulnerable Consumers*. Basic and Applied Social Psychology 36(3):272-279. DOI: 10.1080/01973533.2014.903844

Shearlock, L. & Cambridge, P. (2009). *Working effectively with the police in safeguarding vulnerable adults: sharing experience from Somerset.* The Journal of Adult Protection, Vol. 11 Issue: 4, pp.6-19. Published by Emerald Insight and available at https://doi.org/10.1108/14668203200900024

Smith, W. & Swann, J. (2016). College of Policing Vulnerability Conference Presentation. Available online at https://www.college.police.uk/About/Documents/Conference/The_THRIVE_approach_workshop.pdf

Social Care Institute for Excellence (2016). *The Care Act: safeguarding adults.* Article last updated December 2016. Available online at https://www.scie.org.uk/care-act-2014/safeguarding-adults/

Stockton, G (2018). The Impact of Occupational Fraud on Small Business. Experian.com. Article dated 27th August 2018. Available online at http://www.experian.com/blogs/small-business-matters/2018/08/27/the-impact-of-occupational-fraud-on-small-business/

Sussex Police (2018). *Operation Signature.* Available online at https://sussex.police.uk/advice/protect-yourself-and-others/fraud/operation-signature/

Tapley, J. (2005). *Public Confidence Costs – Criminal Justice from a Victim's Perspective.* British Journal of Community Justice, 3 (2) pp. 25-37.

Tapley, J. (2016). Sharing and collaborating: improving outcomes for victims of crime. Papers from the British Criminology Conference, 16, 111-128

Twitter (2018). Profile of @CityPoliceTell2. Available online at https://twitter.com/actionfrauduk/status/1064449829617762304?lang=en-gb

UK Finance (2018). *Why the Banking Protocol matters.* UKFinance.org.uk. Available online at https://www.ukfinance.org.uk/news-and-insight/blogs/why-banking-protocol-matters

Victim Support (2019). *Victims Code*. Available online at https://www.victimsupport.org.uk/help-and-support/your-rights/victims-code

Walklate, S. (2007). *Imagining The Victim Of Crime.* Published by McGraw-Hill Education

Walklate, S (2017). *Handbook of Victims and Victimology (2nd Ed).* Published by Routledge. https://doi.org/10.4324/9781315712871

Wedlock, E., & Tapley, J. D. (2016). *What works in supporting victims of crime: a rapid evidence assessment*. Crown Copyright.

Whitty M. T. (2018). *Do You Love Me? Psychological Characteristics of Romance Scam Victims*. Cyberpsychology, behavior and social networking, 21(2), 105–109. doi:10.1089/cyber.2016.0729

Wikipedia (2019). List of police forces of the United Kingdom. Page last edited 15th April 2019 and available online at https://en.wikipedia.org/wiki/List_of_police_forces_of_the_United_Kingdom

Wolfgang, M. (1957). *Victim Precipitated Criminal Homicide*. Journal of Criminal Law and Criminology, Volume 48, Issue 1, Article 1. Available online at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4565&context=jclc