THE POLICE FOUNDATION

The UK's policing think tank

perpetuity research

MORE THAN JUST A NUMBER:

IMPROVING THE POLICE RESPONSE TO VICTIMS OF FRAUD

DECEMBER 2018

MORE THAN JUST A NUMBER:
IMPROVING THE POLICE RESPONSE TO VICTIMS OF FRAUD

MICHAEL SKIDMORE, JOSEPHINE RAMM, JANICE GOLDSTRAW-WHITE, CLARE BARRETT, SABINA BARLEAZA, RICK MUIR AND MARTIN GILL

DECEMBER 2018

ISBN: 0-947692-69-X

Acknowledgements

This study would not have been possible without the generous support of the Dawes Trust, to whom we are extremely grateful. The views expressed in this report are solely those of the authors.

We would particularly like to thank PCC Sue Mountstevens and Chief Constable Andy Marsh in Avon and Somerset, PCC Matthew Scott and Chief Constable Alan Pughsley in Kent, PCC Roger Hirst and Chief Constable Stephen Kavanagh in Essex and Commissioner Ian Dyson at the City Of London Police for allowing us to conduct research in their respective forces. Without their full commitment, this study would not have been possible.

We would also like to extend our gratitude to the many practitioners that gave up their valuable time to give us the benefit of their knowledge and experience. The analysts, who patiently worked with researchers to produce valuable datasets, are particularly appreciated, these include the National Fraud Intelligence Bureau, Cifas and Victim Support.

The team would also like to express their gratitude to all those who attended meetings of the National Advisory Board, whose feedback and insight has been invaluable.

About the authors and organisations

This project was conducted by Michael Skidmore, Josephine Ramm, Dr Janice Goldstraw-White, Clare Barrett and Sabina Barleaza under the direction of Dr Rick Muir (The Police Foundation) and Professor Martin Gill (Perpetuity Research).

The Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Its mission is to generate evidence and develop ideas which deliver better policing and a safer society. It does this by producing trusted, impartial research and by working with the police and their partners to create change.

Perpetuity Research

Perpetuity Research is a company that undertakes research in areas of policing and crime, including organised crime. Previous work includes research on money laundering, fraud and corruption, retail theft, identity theft and the illicit market. Perpetuity Research aims to bridge the gap between theory and practice and has produced a range of high profile studies as well as toolkits.

CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

Fraud is estimated to make up 31 per cent of all crime in England and Wales, with 3.24 million fraud offences estimated to have taken place in the twelve months to March 2018. Research has found that 45 per cent of fraud victims felt that the financial loss they experienced had an impact on their emotional wellbeing and 37 per cent reported a significant psychological or emotional impact.

Despite the scale and impact of the problem, it is widely agreed among policymakers, academics and law enforcement officials that fraud and the harms it causes are not prioritised by the police. This study is intended as a response to this imbalance between the scale and impact of fraud and the response it receives from policing. Its aim is to achieve a better understanding of the police response to fraud, to consider how appropriate this is and to suggest how policy and practice could be improved.

To achieve this aim, the research set out to answer the following questions:

- How is the police response to fraud organised across national, regional and local agencies?
- How do police forces and partner agencies prioritise fraud?
- Who is affected by fraud and what support is available to them?
- How do the various organisations and agencies work together to respond to fraud and what roles and powers do they have to achieve this?
- What impact has the internet had on the nature and volume of fraud?
- What is being done to protect victims and identify vulnerability in local areas?
- What determines whether the response to fraud is effective or not and what are the barriers to this?
- Are there examples of emerging good practice which, if replicated, would improve the overall effectiveness of the response to fraud?

In order to gain a full understanding of the subject, the research looked at the fraud response from both a local and national perspective. The majority of the locally based research was conducted in three police force areas – Avon and Somerset, Kent and Essex. Work included interviews with local practitioners, analysis of local data sets and a survey of the local police workforce. The research also included interviews with regional and national stakeholders, a survey of fraud leads across police forces across England and Wales and analysis of national fraud data sets.

THE FRAUD CHALLENGE

Before looking at the police response to fraud in greater depth we describe the nature and complexity of modern fraud. The growth of the internet and its reach into all aspects of life has meant that fraud has moved from being a corporate 'white collar' crime dealt with by specialist law enforcement units to a volume crime affecting millions of individual victims, many of whom expect a local policing response similar to that taken in response to other types of crime.

However, despite the vast scale of fraud affecting England and Wales, the policing and criminal justice response remains limited by comparison. In 2017-18 while 277,561 frauds were reported to the police, only 8,313 cases that year resulted in a charge/summons, caution, or community resolution, representing just three per cent of police recorded fraud.

The rise of volume fraud is linked to the spread of the internet and digital technology. 54 per cent of frauds reported in the Crime Survey for England and Wales have a link to cybercrime. We found that 69 per cent of fraud cases passed on to police forces for investigation in 2016-17 had at least one indicator of cybercrime and 43 per cent involved first contact with the victim being made online.

Related to this strong link to cybercrime, most fraud is committed across local police force borders. We found that 78 per cent of frauds passed on for investigation in 2016-17 involved a victim and a suspect located in different police force areas.

Fraud victims look different from the victims of other types of crime, although patterns of victimisation vary by type of fraud. Overall, fraud victims are more likely to be middle aged, earn more than £50,000 a year, live in a rural or an affluent area and work in a professional or managerial occupation.

There is a common misconception that fraud is a 'victimless' crime. However, fraud can have a significant

emotional and psychological impact on a victim. We found that 35 per cent of victims of frauds, whose cases were passed on for investigation by a police force in 2016-17 reported that the crime had a severe or significant impact upon them.

ENFORCEMENT

The effectiveness of police enforcement

How effective is police enforcement action against fraudsters? Judged by conventional criminal justice outcomes the response does not look good. The overwhelming majority of fraud offences do not result in a conviction. While 3.2 million frauds were estimated to have taken place in 2017-18, just 638,882 frauds were recorded by the police and industry bodies. For every crime reported just one in 13 was allocated for investigation and in that same period only 8,313 cases resulted in a charge/summons, caution, or community resolution, representing just three per cent of the number reported to the police.

This three per cent success rate compares poorly to other types of crime. For example in the year to March 2018 a charge/summons or out of court resolution was achieved for 15 per cent of violent offences, six per cent of sexual offences, nine per cent of robberies, nine per cent of thefts and 13.5 per cent for all police recorded offences.

Fraud investigations take much longer than most other criminal investigations. The average length of time from reporting to charging for fraud offences was 514 days compared to just 50 days for theft offences. There is some good news, however. Court data shows the conviction rate for frauds that reach the criminal courts has remained steady over the past three years, despite increased volumes.

How much variation is there between police forces in the outcomes achieved? The short answer is that we do not know because of major gaps in the data reported by police forces to the National Fraud Intelligence Bureau (NFIB). 52 per cent of crimes allocated for local investigation in April to September 2016 had no recorded criminal justice outcome 12 months later, much of which is due to an absence of proper reporting. The variation in positive outcomes ranges from 79 per cent in one force to zero in two others, but these figures have more to do with an inconsistent approach to recording fraud investigation outcomes than to any real difference in effectiveness.

Recommendation 1: Those responsible for fraud investigations, including police forces or regional units, should be required to monitor and record the outcomes of fraud investigations in a consistent way, according to a template developed by the National Fraud Intelligence Bureau.

The complexity of fraud

The high rate of attrition and the length of time it takes to investigate fraud are due in part to the complexity of fraud investigations. Our analysis of fraud case files found a number of challenges encountered in the course of fraud investigations including locating suspects, gathering evidence and engaging victims.

The process for allocating frauds for investigation

Another cause of lengthy investigations and poor outcomes is the process for allocating cases for investigation. Fraud is unique in policing with the decision-making around when to investigate and where to allocate investigations falling primarily to a national unit (the National Fraud Intelligence Bureau – NFIB), whereas the operational response falls to local policing. While it is important to develop a national picture of fraud offending via the NFIB there are a number of weaknesses in the process of case allocation:

- Decision-making is dependent on the quality of the information provided by victims via Action Fraud but there are significant gaps in this information.
- It takes on average 54 days between a fraud being reported to Action Fraud and a case being allocated for investigation. This can disappoint victims and lead to their disengagement. It also means investigative opportunities can be lost, particularly where the offender is local and a direct report to the force could have been treated as a call for service.
- The police currently lack an effective framework for differentiating one fraud from the next. For most incidents police resource is prioritised based on an assessment of harm but there is no framework in place to identify the harm resulting from fraud.
- The understanding of the problem, which rests with the NFIB, is divorced from the operational response, which rests with local policing. This makes for inconsistent and inefficient decision-making. We found a lack of clarity around who is responsible for a fraud investigation, with some in police forces viewing the crime as being ‘owned’ by the NFIB. This means that professional ownership of a case is diluted. Moreover, the decisions of the NFIB are detached from the considerations of police practitioners on the ground working to distinct local priorities and pressures.

Recommendation 2: There should be a review of all fraud data collected and analysed by the National Fraud Intelligence Bureau with the aim of improving the assessment and allocation of crimes for investigation. In particular the review should aim to improve the quality of the information provided by victims to Action Fraud.

Recommendation 3: The National Fraud Intelligence Bureau should develop a threat and harm index for fraud. This should be used by forces and/or regional units to guide both strategic and tactical decisions.

Local operating models

Police forces use different operating models for managing local fraud investigations. Most forces manage fraud through their general investigative resource, but police officers and staff told us that generalist officers lack the capacity and the capability to investigate fraud effectively. Models which pass all fraud investigations through a dedicated hub appear more promising. While this means a lot of cases are screened out due to limited capacity, dedicated teams can develop the skills to investigate cases more effectively and efficiently. We make a major recommendation on which bodies should take responsibility for investigations in Chapter Six.

THE EXPERIENCE OF FRAUD VICTIMS

Victims' expectations of the system

What do victims of fraud want from the police and the wider criminal justice system? Research has found victims are most concerned about getting their money back and seeing the offender convicted. Given the complexity of fraud and its generally cross-border nature these outcomes are unlikely to be achieved in most cases. However, victims also value a number of other more achievable outcomes: having a single point of contact, receiving a sympathetic and understanding response, having someone to listen to them and having support to get over the experience. We found that these expectations are far from being met in practice.

Reporting fraud

While a central reporting hub is important to provide a national perspective on a cross-border problem and to support rational resource allocation, there are a number of challenges with the way Action Fraud works:

- There is still confusion among the public about where to report fraud, with fewer than five per cent naming Action Fraud as the place they would be most likely to report to and 48 per cent still saying they would report it to their the local police.
- Action Fraud does not have the capacity to manage the current number of calls it receives.
- The way in which Action Fraud identifies risk and vulnerability among victims is too subjective and is not consistent.
- The process for signposting victims for further advice, resolution or support can be confusing, with victims being passed around a multitude of services to get the resolution they need.
- Once a report is submitted to Action Fraud either online or on the phone, the information victims receive is minimal and subject to considerable delays.

Recommendation 4: The City of London Police should be given more resources so that it can handle more calls and provide an improved service to victims

Recommendation 5: The Action Fraud website should provide more authoritative advice and information to guide victims through the services available. It should make online interaction easier, including providing remote advisors who can assess and refer victims where appropriate. It should provide a way for victims to track their case through the system and remain informed about its progress.

Recommendation 6: All bodies collecting fraud reports (Action Fraud, the local police, third and private sector bodies) should work to minimum service standards that cover victims' basic expectations. These standards should be clearly communicated to victims. Given the scale of under reporting, these communications should also make clear the value of victims submitting a crime report.

Many people continue to report fraud directly to local police forces, although 59 per cent of police forces who responded to our survey reported that they did not monitor how many fraud victims contact them directly and a further two forces (six per cent) reported that they did not know if this was something they monitored. The response from forces is inconsistent across the country and some forces are not properly considering whether some of these direct reports ought to be treated as a call for service (for instance if the victim is vulnerable or if the offender was physically present).

Recommendation 7: There should be clear national guidance on what police forces should do when they are initially contacted by a victim of fraud. This should ensure that victims are assessed to

determine whether or not their report should be treated as a local call for service, for example, if the victim is vulnerable or if a local offender is suspected.

The many organisations that receive fraud reports operate largely in isolation from one another and form a landscape of services that is complex for victims to engage with.This both discourages fraud reporting and makes it difficult for the organisations that are involved to respond effectively to fraud.

Recommendation 8: The public should be made aware of the different reporting channels, and in what circumstances they should be accessed, so that they can access the service most appropriate to their needs

Victims services

The service victims receive from the police varies considerably by force. 47 per cent of forces told us that all or most fraud victims who contact them are simply referred to Action Fraud. 20 per cent of police forces told us that they visit all or most fraud victims who make direct contact with them.

Most victims, once they have reported to Action Fraud, are presented to their local police in the form of a list issued by the National Fraud Intelligence Bureau on a monthly basis. The majority of the victims on this list will not receive a police investigation. 69 per cent of forces offer some kind of service to these victims based on eligibility criteria, usually related to whether the victim was vulnerable. 28 per cent of forces offer no service at all.

Victims who are allocated an investigation may be contacted by an investigator, normally in another force, leading on their case. Managing victims remotely in this way can be challenging for local police investigators and the approach varies across the country.

Recommendation 9: There should be a national minimum standard of service available to all fraud victims whose cases are being investigated.

All victims of crime have a right to access victim support services to help them recover from the effects of a crime. Action Fraud offers this service when victims report a fraud and this is delivered by a local provider. In 2016-17 35, 220 victims took up this offer but 89 per cent chose not to engage when contacted by the local provider. Practitioners told us that victims generally did not want the support offered by generic victim support services and that staff are not provided with training on the needs of fraud victims. They also told us there are considerable time lags between referral and support being offered.

Recommendation 10: Action Fraud should make clear to victims what they can expect from when they are referred to a local victim support service.

Support for vulnerable victims

There is an increasing recognition of the additional needs of vulnerable people in relation to fraud. Analysis of current Police and Crime Plans found a reference to vulnerable fraud victims in 40 per cent of the plans. Our national survey of police leads for fraud showed the characteristics and experience of the victim to be the most important factors for determining the provision of victim services.

Recommendation 11: There should be a national framework, for identifying, assessing and prioritising fraud related vulnerability. All police forces, regional units and Action Fraud should use the same criteria.

Recommendation 12: All fraud victims who are identified as vulnerable should receive at the very least, a follow up call from their local police force.

Recommendation 13: The Home Office should fund an expansion of the Economic Crime Victim Care Unit to cover all police forces to provide a baseline of sustainable provision for identifying, assessing and supporting vulnerable victims of fraud. The Unit should make referrals to the local police force for further action where appropriate.

PREVENTING FRAUD

There is a consensus among police practitioners that, while enforcement is important, we cannot ‘arrest our way’ out of the fraud problem. Prevention is critical in tackling a volume crime like fraud.

Much fraud prevention work in the UK has focused on raising the public’s awareness of risk so that people and organisations can better protect themselves. However it is hard to measure the effect of these various campaigns and there is some evidence that the multiplicity of services and initiatives may be confusing for the public.

Recommendation 14: The Joint Fraud Task Force should coordinate and consolidate the messaging from fraud awareness campaigns delivered across the public and private sector.

Recommendation 15: The Home Office should commission research to examine the effectiveness of public awareness campaigns for fraud and cybercrime prevention. The research should produce recommendations for more coordinated and targeted delivery of these communications.

There is also a lack of coordination of local prevention efforts. Our analysis of police and crime plans found that, although several highlighted prevention or early intervention they provided limited details about what this entails. Local strategic partnerships for delivering prevention were either absent or delivered on the basis of fixed-term resourcing. There is a lack of clarity around roles and responsibilities of different agencies and therefore poor coordination of messaging and effort.

Recommendation 16: Police officers should be trained in how to deliver effective fraud and cybercrime prevention messages and local policing teams should provide this advice as routinely as they give out other crime prevention messages.

Recommendation 17: The local fraud data provided to police forces by the National Fraud Intelligence Bureau should be presented in a way that helps local police forces understand their specific fraud problems and the characteristic of local victims. This will ensure that forces are better placed to develop targeted prevention advice and take a problem solving approach, particularly for fraud carried out by local offenders on local victims.

Recommendation 18: Serious and persistent fraudsters (including those involved with known organised crime groups), vulnerable groups and victims, as well as emerging systemic vulnerabilities should be incorporated into police profiles of the local serious and organised crime threat. The assessment should be developed collaboratively by the police, local authorities, third sector and local business representatives, and used to support targeted local prevention strategies.

Recommendation 19: Police and Crime Commissioners should establish fraud prevention partnerships or at least explicitly include fraud and cyber prevention work within existing local crime prevention partnerships and strategies. The plans developed by these partnerships should be clear about who will be leading on local fraud prevention work, and what this will involve.

Fraud is still under-reported, in particular by the private sector. Victims are not encouraged to engage with the authorities due to a lack of clarity about the importance of reporting fraud, the information they need to provide and the action that will be taken after they have reported it.

Recommendation 20: Consolidating fraud intelligence data from across the public and private sectors should be an ambition for the government. This would augment current capability to identify offenders, recognise vulnerability and emerging threats, and direct public resource to where it is most needed. As a first step there should be a stock-take of information collected by different bodies and an analysis of how this information can be effectively integrated and applied to fraud policing.

BUILDING A BETTER SYSTEM FOR TACKLING FRAUD

While this report has highlighted examples of good practice it is clear that overall the police response is falling short of where it ought to be if we are to catch or disrupt fraudsters, support victims and prevent fraud. So far we have identified a range of problems within three different parts of the response: enforcement, the service provided to victims and prevention. Behind these operational failings is a deeper problem: we simply do not prioritise tackling fraud across the UK, and consequently the national law enforcement system we have put in place to tackle it is inadequate.

Should we prioritise fraud?

When asked about which offence types should be among the top three priorities for policing 61 per cent of the public said violent crime, 54 per cent said terrorism/extremism and 49 per cent said rape and other sexual offences. Only four per cent mentioned fraud, making it a lower priority for the public than online abuse and drug offences. Given the public's lack of concern, it is not surprising that politicians and the police do not prioritise fraud. Should they?

Given the range and seriousness of the demands on the police and in the context of recent budget cuts it is understandable that fraud has not received greater strategic focus. However, we can be realistic about what can be achieved, while also recognising that fraud deserves greater attention from policy makers and law enforcement agencies.

There are three reasons for this:

- Although the level of harm is not well understood at the individual level, the aggregate harm caused by fraud is considerable. Fraud is estimated to cost the UK £190 billion a year, with £6.8 billion as a result of fraud that directly targeted individuals. The UK loses more financially every year to fraud compared to most other types of organised crime. These are not just real losses to families and businesses, but they also result in funds being channeled out of the UK and into the criminal economy.
- Preventing and investigating fraud is part of a strategy for dealing with other types of crime.

Fraud is closely connected with other aspects of organised criminal activity, notably cybercrime (and associated identity theft), money laundering, corruption and counterfeiting.

- Around a third of victims of fraud say they have suffered a significant emotional or psychological impact as a result.

We are not naive about the resource pressures on policing and law enforcement. In our recommendations below, we argue that there are structural and workforce reforms that should improve efficiency as well as effectiveness. But ultimately if the government wants law enforcement to investigate fraud more effectively, as well as prevent it and provide a better service to victims, it will inevitably have to find more money to deliver this.

Governance and strategy

Fraud is one of the most pervasive crimes in the UK, affecting more than three million people a year, and yet there is no national strategy for dealing with it. The last national strategy for tackling fraud was published in 2011 by an agency that no longer exists and our research found few practitioners made reference to it.

Recommendation 21: The government should produce a national, cross-departmental strategy for tackling fraud alongside a specific national fraud policing strategy.

This absence of a national strategic focus on fraud means there is weak accountability throughout the system for tackling this important area of economic crime. Accountability among the national agencies is dispersed. The National Crime Agency does not work directly on fraud and is not responsible for the operational response even though it does have responsibility for serious and organised crime which is widely acknowledged to include fraud. The City of London Police is the national lead police force but the operational policing response sits locally and the lead force has no power to hold local policing to account for their performance in tackling fraud.

Nor is fraud prioritised locally. Although 74 per cent of police and crime plans mention fraud, 26 per cent do not. Fraud does not feature in a number of key strategic assessments locally which have a particular focus on serious and organised crime and which help to steer local resourcing and priorities.

Recommendation 22: The Home Office should be responsible for overseeing the implementation of the national fraud strategy. The City of London Police should be responsible for ensuring delivery of the national fraud policing strategy.

Recommendation 23: The Strategic Policing Requirement should be much more explicit about how local forces are expected to approach fraud and cross border crime generally. HMICFRS should inspect against this expectation.

Given the low prioritisation of fraud politically at both national and local levels it is not surprising that we find major gaps in the performance management architecture:

- Police forces do not monitor and record the outcomes of fraud investigations in a consistent way (see Recommendation 1).
- In the official statistics there is little differentiation of frauds in terms of complexity, seriousness or harm. This makes it hard to judge whether forces are using their resources in an efficient and effective way (see Recommendation 3).
- Arguably, forces are still measuring the wrong things. Even though we were told in our interviews with practitioners and experts that traditional criminal justice outcomes should not be the primary focus, effectiveness is still largely measured by those outcomes.
- The police share responsibility for tackling fraud with an expansive web of statutory, private and third sector organisations but there is very little measurement of and accountability for their response to fraud.

Recommendation 24: Forces and regional units should be required to report back to the National Fraud Intelligence Bureau not just on criminal justice outcomes but also on victims services, prevention work and disruption activity.

Recommendation 25: the Joint Fraud Taskforce should agree on how the performance of the private sector and other partners will be measured in relation to fraud and then report annually on those measures.

Structure

Fraud presents a major challenge to the way in which policing and law enforcement is structured in England and Wales. It is a cross-border crime mostly dealt with by a fragmented and localised police service. Centralised reporting and analysis through Action Fraud and the National Fraud Intelligence Bureau is vital to gaining a national perspective on a cross border crime. However, currently this means that the understanding of the problem is divorced from the operational response.

These two aspects need to be brought together via a reallocation of roles and responsibilities.

Recommendation 26: The way in which the police response to fraud is structured needs to change:

- ***Nationally, the City of London Police should continue to provide the central reporting hub (Action Fraud) and the national intelligence centre (the National Fraud Intelligence Bureau);***
- ***Fraud investigations should no longer be the responsibility of local police forces and all investigations should be handled by regional fraud investigation units that would exist alongside the Regional Organised Crime Units. This network of regional units should be coordinated and tasked by the City of London Police. Where the fraud is assessed as serious or complex it should be escalated into the Economic Crime Centre within the National Crime Agency for national tasking;***
- ***There should be a national service for vulnerable victims made possible through an expanded Economic Crime Victims Care Unit (ECVU), which can then make referrals into local services;***
- ***Local policing should be responsible for responding to local frauds treated as a call for service, providing local fraud prevention advice and contacting and supporting vulnerable victims in their areas who are referred via the ECVCU.***

Workforce

Is the police workforce organised in such a way to effectively deal with fraud? Previous research has used investment in specialist Economic Crime Teams as a barometer for the level of police commitment to tackling fraud. Our analysis shows that in 2017 there were 1,455 (0.8 per cent) full-time equivalent police personnel working in Economic Crime Teams across England and Wales, 46 per cent of whom were civilian staff. This degree of resourcing is tiny when compared to the scale of fraud. It is worth noting that Economic Crime Teams have a remit beyond fraud, including financial investigation to deal with money laundering and asset recovery in relation to all crime.

In addition to capacity issues within these specialist teams there is a concern about recruitment and retention of fraud specialists. A third of police force leads reported they were not confident they could recruit the right staff to tackle fraud and a quarter were not confident in being able to retain them.

In 69 per cent of forces all or most fraud investigations are dealt with by generalist officers, despite the fact that 69 per cent of strategic fraud leads believe that the lack of knowledge in the workforce was one of the most challenging factors in delivering local fraud investigation. 81 per cent of officers and staff surveyed agreed that fraud policing requires a different set of skills to other crimes, 78 per cent considered that they needed more training to deal with fraud and 86 per cent believed it should be dealt with by specialists. There is a capacity as well as a capability problem: 74 per cent disagreed that they had enough time to deal with a fraud case or victim.

There are a number of reasons why it is more effective and efficient for fraud investigations to be handled by dedicated teams:

- Fraud investigation is different from most other types of local crime investigation and requires a set of skills and relationships that generalist officers do not possess.
- Most fraud investigations are desk based and do not require the same kind of physical presence necessitated during other local investigations.
- Dedicated teams of fraud investigators would build up skills, knowledge, networks and overall capability so that they could investigate frauds more quickly and effectively.
- Even if the number of frauds investigated under this system is fewer than at present we believe that it is better to undertake a smaller number of successful investigations than it is to take on a larger number, most of which are not prioritised or successful.

Recommendation 27: All fraud investigations should be handled by dedicated investigators, housed mainly in regional fraud investigation units. These would include specialists currently working in Economic Crime Teams leading on large and complex fraud, and volume fraud that is currently allocated to non-specialist officers. Many of these investigators would not need to be police officers and could be recruited via different channels.

1. INTRODUCTION

1.1 BACKGROUND

Findings from the Crime Survey of England and Wales estimate there were 3.24 million fraud offences for the year ending March 2018 (Office for National Statistics, 2018a). Fraud now makes up 31 per cent of all crime reported in the survey. However it has become apparent that despite the scale and impact of fraud, it is generally not prioritised by policymakers or the police. Reporting rates (both by the public and businesses) are low; the enforcement response has been deemed wanting (Button et al, 2012; Doig and Levi, 2013), and the harms caused to people by fraud, and victims' subsequent needs, have received little attention from the police or other services (Cross, 2015; Button and Cross, 2017).

In previous research (Crocker et al, 2017), the Police Foundation and Perpetuity Research reported a number of striking findings about how organised fraud was treated by local police teams:

- Fraud was largely absent from policies and resources for tackling organised crime.
- There was very little prioritisation of enforcement, victim support, or prevention within police forces.
- There was a considerable disconnect between, on the one hand the national intelligence and coordination teams, and on the other, what was being delivered on the ground.

Overall, the response to fraud was found to be variable in quality and consistency and our report recommended that a full-scale review be carried out to assess how fraud that impacts local victims is policed (ibid).

Recently, there has been a shift in police attention away from volume crime and towards harm reduction (Hales and Higgins, 2016). Offence types such as child sexual exploitation and modern slavery present new challenges and have attracted focus and resource. As a 'volume' crime, and one that has for a long time been encumbered with the perception of being victimless and low-harm, fraud has struggled to receive much attention within this new vulnerability landscape. Indeed, for the police, fraud generally falls under the umbrella of economic crime, which is neither prioritised locally nor within regional or national efforts to tackle organised crime (Doig and Levi, 2013).

This study is intended as a response to this imbalance between the scale and impact of fraud and the response it receives from policing. Its aim is to understand the quality of the police response to fraud and to suggest ways to improve it.

In embarking on this research we were not naive about the pressures on police resources. Local constabularies are under significant strain, having to deal with rising areas of complex demand at the same time as they have experienced a 20 per cent loss in resources in real terms. In this context fraud is always likely to struggle against other priorities. However it is also our belief that the response to what is now the second largest 'class' of crime after theft (Office for National Statistics, 2018a), can and should be improved.

1.2 THE AIMS OF THIS STUDY

The overarching aim of this study is to contribute to a better empirical understanding of the police response to fraud, to consider how appropriate it is and to suggest how future practice could be improved. To achieve this aim, the research set out to answer a series of questions, including:

- How is the police response to fraud configured across national, regional and local agencies?
- How do police forces and partner agencies prioritise frauds?
- Who is affected by fraud and what support is available to them?
- How do the various organisations and agencies work together to respond to fraud and what roles and powers do they have to achieve this?
- What impact has the internet had on the nature and level of fraud?
- What is being done to protect victims and identify vulnerability in local areas?
- What determines whether the response to fraud is effective or not and what are the barriers to this?
- Are there examples of emerging good practice which, if replicated, would improve the overall effectiveness of the response to fraud?

1.3 METHODOLOGY

The project used a mixed-methods approach, employing a variety of qualitative and quantitative research methods to answer the research questions set out above. In order

to gain a full understanding of the subject, the research took both a local and national perspective:

- The majority of the local research was conducted in three police force areas – Avon and Somerset, Kent, and Essex. Work included interviews with local practitioners, analysis of local data sets and a survey of the workforce;
- The national level research included interviews with regional and national stakeholders, a survey of fraud leads across police forces across England and Wales, and analysis of national fraud data sets.

The methodologies are described in Table 1 below.

TABLE 1: An outline of research methodologies. [1]

Source	Description of the evidence
Practitioner interviews	Through a series of 107 meetings and interviews, 117 practitioners were engaged (a number of interviews included more than one practitioner). The interviews were conducted with local, regional and national practitioners in the police, the government and partner agencies, as well as in the third and private sector.
National police force survey	The strategic lead officers for fraud in all England and Wales police forces were surveyed on how the response to fraud is structured in their local area: key themes were strategy, investigation, victim care and workforce. Out of 43 police forces, 32 completed and returned a survey.
Police workforce survey	An attitudinal survey was sent to police officers and staff in Kent, Essex and Avon and Somerset. Key themes included prioritisation, capability and challenges as perceived by practitioners across all levels and functions. A total of 405 surveys were completed, the majority from Essex (n=211) and Kent (n=95) with a small number from Avon and Somerset (n=23) [2].
Trading Standards offices survey	All UK Trading Standards offices were surveyed for qualitative insights on how they structure their response to fraud victims, local partnership arrangements and local initiatives. Data was received from 21 Trading Standards offices.
National fraud data	National data for all frauds allocated an investigation or other response by City of London Police in the financial year 2016/17 were analysed. This data included a total of 64,857 crimes allocated in this period. National data for all fraud victims disseminated to police forces in England and Wales by City of London Police were also analysed. This data included a total of 223,701 victims of fraud.
Local crime data	Crime data from Avon and Somerset and Essex police were collected for the two year financial period 2015-17. In-depth analysis was completed for 25 fraud investigation case files from Avon and Somerset. A purposive sampling strategy was employed to capture the range of frauds, investigating practitioners and outcomes.
Literature review	This incorporated published articles from academia, the public sector, the government and other relevant stakeholders. The literature also included non-published strategic assessments and documentation from within the police and other organisations (such as Cifas and Victim Support).

[1] Please see Appendix A for a full description of the methodologies.

[2] 76 respondents did not specify which police force they were from.

1.4 REPORT STRUCTURE

The report is structured as follows.

In Chapter 2 we set out the context in which this report sits. We describe what fraud is and distinguish between different types of fraud. We briefly lay out the history of how fraud has been viewed and tackled by the government and law enforcement. We then set out the scale of fraud today and show how much of fraud is now linked to cybercrime. We examine the extent to which fraud is now a crime that crosses regional and national borders. Finally, we describe the characteristics of the victims of fraud and assess its impact upon them.

In Chapter 3 we look at fraud enforcement activity by the police, assessing its overall effectiveness. We show how few fraud cases result in positive criminal justice outcomes and look at data comparing the effectiveness of different police forces in relation to fraud enforcement. We argue that these poor outcomes are in part down to the intrinsic complexity of fraud investigation. We also show that these outcomes are a result of deficiencies in the process of case allocation. In particular we highlight the problems that emerge because of the separation of those responsible for understanding the problem from those responsible for the operational response. We finally describe a number of different models for managing fraud investigations and identify examples of good practice.

In Chapter 4 we discuss the service provided by the police to victims of frauds. We set out what victims of fraud expect from the police and the criminal justice system. We then go on to describe and assess the processes of reporting fraud and the services available to victims.

In Chapter 5 we look at what is being done by the police and their partners to prevent fraud both locally and nationally.

In Chapter 6 we explain the weaknesses identified in enforcement, victim care and prevention activity with reference to the wider national system for tackling fraud. We look in particular at strategy and governance, the structure of the operational network and the deployment of the police workforce in tackling fraud. We conclude with a number of recommendations for reform to deliver a step change in the police response.

2. THE FRAUD CHALLENGE

This chapter describes the nature and impact of fraud. We begin by defining fraud and describing its component parts. We go on to describe how the response to fraud in England and Wales has changed over time. We then set out the scale of fraud, the scale of the police response, the relationship between fraud and cybercrime, the degree to which fraud is a cross border crime, the characteristics of fraud victims and the impact of fraud upon them.

2.1 WHAT IS FRAUD?

Fraud is wrongful or criminal deception intended for personal or financial gain. Justice can be pursued either as a civil matter by a victim taking action directly or as a criminal matter by the police and criminal justice system.

Fraud is comprised of a bewildering range of modi operandi, takes place in a diverse range of physical and digital spaces and is directed at many different types of victim. The methods can include offenders that groom and abuse victims within interpersonal relationships (Dalley et al, 2017; Phillips 2017), offenders working to a business model for perpetrating fraud across jurisdictions (Levi, 2008; Lusthaus and Varese, 2017), insider abuse of professions or financial markets (Haynes 2012) and many more besides.

In the current crime classification system there are 48 separate categories of fraud [3] (Home Office, 2018a) [4] which, for simplicity, are grouped in Table 2 on the basis of four characteristics:

- The products or services used by fraudsters to offend.
- The commercial environments in which fraud can take place.
- The industries or sectors in which fraud offending is concentrated.
- The means by which fraudsters make use of positions or occupations to perpetrate fraud (see Appendix B for a complete breakdown by offence code).

TABLE 2: A typology of fraud based on themes in the Home Office offence classification system.

Fraud categorisation	Description
Products or services • Advance fee payments • Financial investments • Non-investment fraud	This encompasses a wide variety of methods that principally target members of the public as consumers or those making investments. The categories are principally differentiated by the range of products or services that are exploited by offenders such as ticket sales, loans and shares. Many categories involve methods of taking advance payment for something that either does not exist or has been misrepresented.
Commercial environment • Online shopping and auction • Retail fraud • Business trading fraud • Door to door sales and bogus tradesmen	Frauds categorised on the basis of being perpetrated within specific commercial environments such as online or in retail. They encompass diverse modi operandi but commonly involve methods of taking advance payment for something that either does not exist or has been misrepresented, or fraudulent payments made to a vendor. While these categories include fraud that impacts on individual members of the public, they also include many that target local businesses (for example, retail fraud).
Industry or sector • Banking and credit industry • Insurance fraud • Telecom industry fraud • Pension fraud • Charity fraud • Public sector fraud	These fraud categories are based on particular industries or sectors affected by fraud, many through the abuse of products or services (commonly financial services) by external offenders or by someone holding a position within these sectors. This group also includes categories in which service users can be victimised, such as the use of stolen identity or finance details or misrepresentation of products such as pensions or insurance.

[3] There are an additional eight categories for computer misuse offences that are also recorded by City of London Police.

[4] A complete description for each fraud offence category can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694449/count-fraud-apr-2018.pdf [accessed 07.09.2018].

Fraud categorisation	Description
Use of position or occupation • Corporate fraud • False accounting • Bankruptcy and insolvency • Other regulatory fraud • Fraud by failing to disclose information • Abuse of position of trust	This group includes fraud types based on specific social or professional positions (for example a corporate employee, solicitor or business owner) which create opportunities to perpetrate fraud. In this fraud category perpetrators commonly use a trusted position to abuse regulatory systems or financial service providers, or defraud employers, business associates or service users.

* This table does not include the 'Other' category of fraud.

2.2 HOW THE RESPONSE TO FRAUD HAS EVOLVED OVER TIME

Edwin Sutherland was the first to attempt to define fraud, what he termed 'white-collar crime' in 1939, as being an offence committed by people of respectability and high social status, in the course of their occupation (Sutherland, 1983). Following this, there was much debate about whether it should be defined by the offender, or by the act, and whether a legalistic approach was too narrow to define these activities (Blum-West and Carter, 1983). Over the next few decades, definitions were refined to include fraudulent acts committed by corporations, by people of any social status and during everyday life not just through occupational acts.

Over the next few decades, besides continuing debates about definitional aspects, fraud remained on the sidelines of public policy, viewed as an offence that harmed few people and mainly affected big business. A renewed policy focus on corporate governance in the 1990s and the expansion of the internet led to greater political interest in fraud. This resulted in a government led review of fraud, published in 2006 and containing 62 recommendations to reduce fraud and the harm it caused (HM Government, 2006).

The review led to a number of important changes. In response to criticisms that anti-fraud work was fragmented and lacking in coordination, the National Strategic Fraud Authority (NSFA), later renamed the National Fraud Authority (NFA), was created and charged with publishing a national fraud strategy and monitoring its implementation. It had the advantage of being able to push ahead with key projects and to bring together of many stakeholders to pursue fraud (Fraud Advisory Panel, 2016). The National Strategy for Fraud was published in 2011 but the NFA was disbanded in 2014.

The Joint Fraud Taskforce was launched in 2016 as a further attempt to achieve greater coordination of anti-fraud stakeholders particularly across the financial sector and law enforcement.

Historically the extent and nature of fraud has been obscure, which itself prevented a strategic response. This is partly due to patchy recording practices by the police, who sometimes did not understand or prioritise the offence. It is also because criminal offences of fraud on the one hand and civil disputes on the other were confused. To address this, a new central reporting body was established following the Fraud Review, later renamed and launched in 2009 as Action Fraud and rolled out nationally in 2013. Its aim was to overcome the issue of under-reporting of fraud and to look at the 'bigger picture' (Fraud Advisory Panel, 2016).

This was supported by the National Fraud Intelligence Bureau, which was created to analyse the reported data and to distribute it in the form of intelligence packages to local police forces. In 2010, the first Annual Fraud Indicator was published to estimate the costs from all fraud to the UK, although this was abolished in 2014. In 2017, fraud and cybercrime were reported for the first time in the Crime Survey for England and Wales (relating to the year to September 2016). The inclusion of these two offence categories led to a near doubling of the total number of crimes reported in the survey.

One of the greatest changes to the legal fraud environment since the Theft Act (1968) and prompted by the Fraud Review, was the introduction of the Fraud Act (2006)[5]. Because fraud stretches over an extensive range of behaviours, contexts and consequences (in terms of who the victims are and the harm caused) the new Act aimed to bring together disparate parts of legislation used to prosecute fraudsters. It introduced a new offence of fraud which could be committed in three ways: by way of false representation (Section 2), failing to

[5] Available at https://www.legislation.gov.uk/ukpga/2006/35/contents [Accessed 18.10.2018].

disclose information (Section 3) and abuse of position (Section 4) (Fraud Act, 2006).

This changed the legal fraud landscape, making complex aspects of the law easier for the police, the public and jurors to understand. In addition, there was a substantial easing of the burden of proof required for both fraudulent acts and deception offences (Betts, 2017). The legal framework in this area was further strengthened by the publication of the Bribery Act in 2010.

These were all steps towards enabling a more robust police response to fraud, albeit they were introduced as the police experienced a sharp squeeze on resources which affected their ability to pursue fraud. One of the changes introduced following the Fraud Review was to make the City of London Police the national lead force for fraud. At the local level fraud has not historically been a priority for the police. As we shall show in the chapters that follow, local police forces have generally not kept pace with a rapidly changing crime landscape, in particular one that has migrated away from the street and into online spaces (Bossler and Holt, 2012; Loveday, 2017).

The growth and ubiquity of the internet has meant that fraud has moved from being a corporate problem to a volume crime affecting millions of individual victims. This brought with it challenges for policing (Levi et al, 2015). Not only did it create a new category of internet-dependent crime, it enabled fraud to be committed on a far greater scale, across many boundaries (including international boundaries), at greater speed and with relative ease, and rendered offenders even less likely to be apprehended, prosecuted and convicted.

At least in part because of the limited service provided by the police, there has been a rise in private and public sector organisations involved in tackling fraud (Button et al, 2016). Cifas and Financial Fraud UK are two of the largest bodies recording frauds affecting business as well as charities and public sector organisations, and together record more fraud in the UK than Action Fraud (Home Office, 2018b). Fraud is complex to investigate and prosecute because there are definitional overlaps between offence categories, and additional legislation is used to regulate specific services or areas of business – for example, legislation against tax or benefit fraud [6], false accounting [7] or consumer protection law [8]. A number of these provide public bodies with specific powers to sanction fraudsters outside of the Criminal Justice System; for example, the Department for Work and Pensions can impose financial penalties on those who defraud the benefits system.

Similarly, the private sector has extra-legal systems for tackling fraud; examples include powers to expel members from professional bodies (eg Solicitors Regulation Authority), staff dismissal or services that block access from suspected fraudsters by placing them on to a 'black-list' register (Button et al, 2016). Many state agencies have developed their own specialist counter fraud resources for example, the NHS has its own intelligence-led organisation, the NHS Counter Fraud Authority, which identifies, investigates and prevents fraud (and other economic crime) within the health service. In short, the police operate within a complex web of agencies and organisations each playing different roles in enforcing regulation, facilitating asset control, aiding public protection or providing services for victims or those at risk.

2.3 THE SCALE AND NATURE OF FRAUD

Fraud and the police response in England and Wales: Key facts

SCALE

3,245,000	fraud incidents were reported by members of the public in 2017-18, 31 per cent of all crime-related incidents experienced by the public in that period.
132 per cent	increase in reporting from the public since 2011/12, when Action Fraud was introduced. Fraud made up 12 per cent of all crime recorded by the police in 2017-18.
57 per cent	of fraud recorded in 2017-18 was reported by industry bodies Cifas and Finance UK.
One in five	frauds were reported to the police compared to more than one in two theft offences.

[6] Value Added Tax Act, 1994; Taxes Management Act, 1970; Customs and Excise Management Act, 1979; Social Security Administration Act, 1992; Tax Credits Act, 2002.

[7] Theft Act (1968).

[8] Consumer Rights Act (2015).

POLICE RESPONSE

One in 13 frauds reported to the police were allocated an investigation in 2017-18.

Three per cent of fraud recorded in 2017-18 led to a charge/summons, caution, or community resolution, falling to **1.3 per cent** if crimes reported by Cifas and UK Finance are factored in [9].

One in 134 employees in the police workforce has a main function recorded as economic crime investigation, and **one in 241** a main function recorded as cybercrime investigation [10].

514 days was the average length of time between an offence and an offender subsequently being charged in 2017, ten times longer than for a theft offence [11].

52 per cent of crimes allocated for police investigation had no recorded update 12 to 18 months later [12].

211,462 victims were referred by Action Fraud to police forces in 2016-17, averaging **17,622** referrals each month. Most were linked to crimes that will not be investigated.

4,918 was the average number of victims referred to a police force in a single year, ranging from 38,038 in the Metropolitan police to 1,404 in Cleveland [13].

Fraud is the most commonly occurring type of crime in the UK. Figures from the Crime Survey for England and Wales estimate that 3.2 million fraud offences were experienced by the public in the year ending March 2018, and 1.2 million computer misuse offences (Office for National Statistics, 2018b).

Only a minority of these frauds were reported to the police or other recording bodies. In total 638,882 frauds were reported in 2017-18, of which 277,561 (43 per cent) were reported to the police, 276,993 (43 per cent) by Cifas and 84,328 (13 per cent) by UK Finance (Office for National Statistics, 2018b). A survey of business premises across a number of industry sectors found that more than one in ten (12 per cent) had experienced fraud over the year but reporting rates were among the lowest of all crimes (Home Office, 2018c). For example, while the majority of people reported burglary (85 per cent) or attempted burglary (71 per cent), less than a third reported fraud by an unknown person (31 per cent).

Reporting has been increasing however. For a number of years fraud has bucked a downward trend in recorded acquisitive crime, as shown in Figure 1.[14] The creation of Action Fraud in 2011 and the integration of crime reports from industry bodies (Cifas and UK Finance) have increased reporting levels and the visibility of fraud to law enforcement.

In terms of the types of frauds reported to the police in 2016-17, 40 per cent fell within the category of frauds relating to specific products or services, 23 per cent were offences defined by a commercial environment (in retail or online for example), 16 per cent referred to fraud affecting a particular industry or sector and just two per cent relate to the use of a position or occupation (See Figure 2). A very large proportion (19 per cent) are categorised as 'other' which is likely to reflect the difficulty victims and practitioners have in understanding the nature of the fraud that has occurred and the large number of categories they have to navigate when reporting.

[9] All figures taken from ONS (2018) Crime in England and Wales: year ending March 2018 and Home Office (2018) Crime outcomes in England and Wales: year ending March 2018.

[10] Data available at https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2018 [accessed 24.10.2018].

[11] Data available at https://www.gov.uk/government/statistics/criminal-court-statistics-quarterly-october-to-december-2017 [accessed 24.10.2018].

[12] This and the figures below are reflective of 2016-17 unpublished fraud data received from the police.

[13] Excluding City of London which is largely non-residential.

[14] It should be noted that in the last two years a number of other types of reported acquisitive crime have been increasing, most notably burglary, robbery and vehicle related theft (ONS 2018).

FIGURE 1: Trends in recorded acquisitive crimes, 1998-2018. [15]

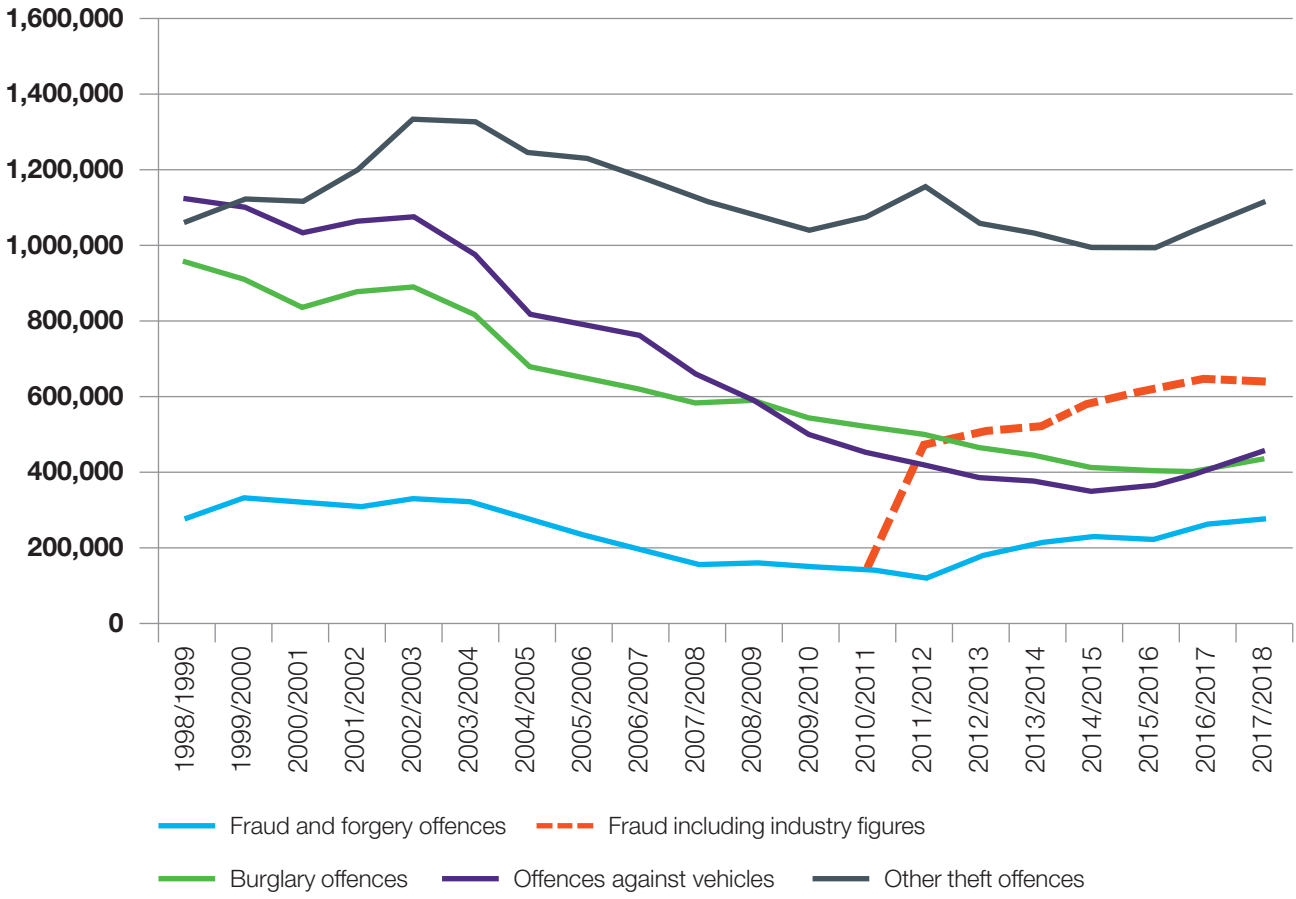
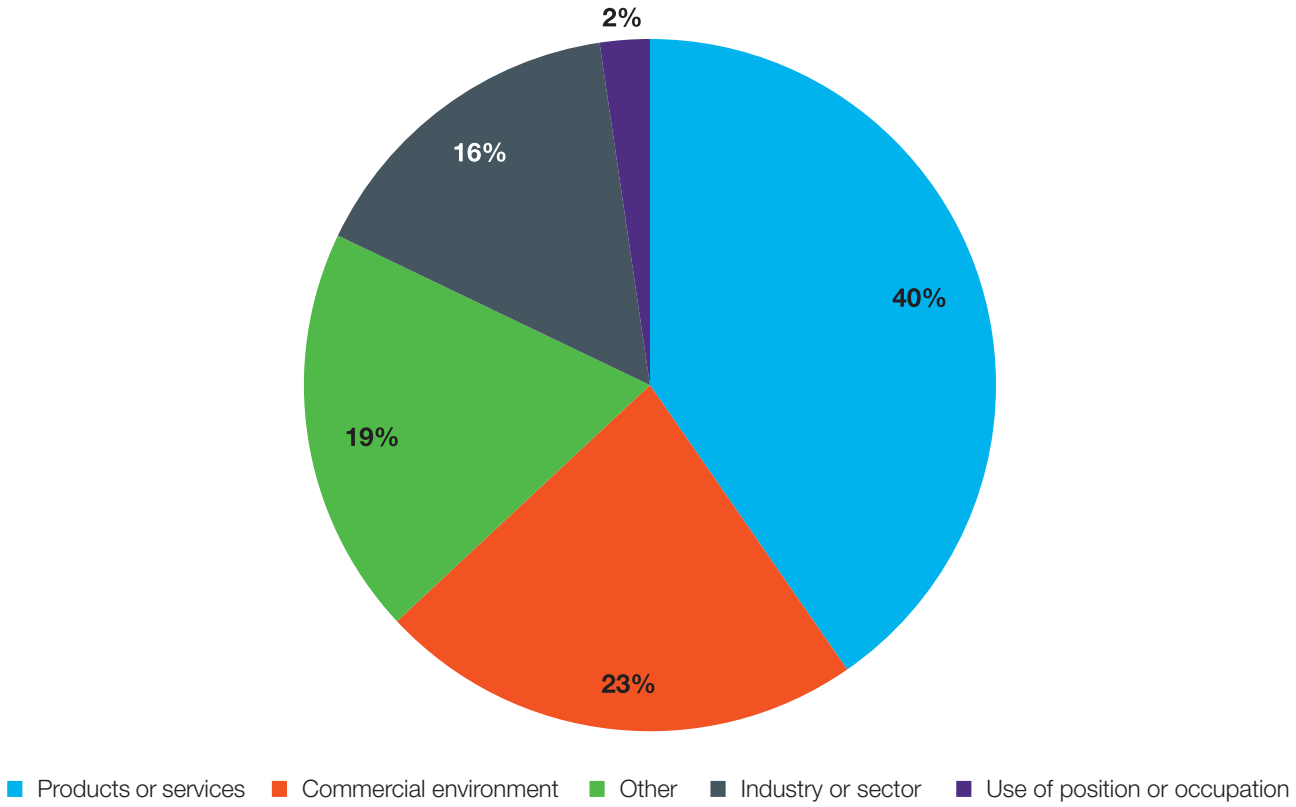


FIGURE 2: An overview of the distribution of fraud categories reported to the police in 2016-17.



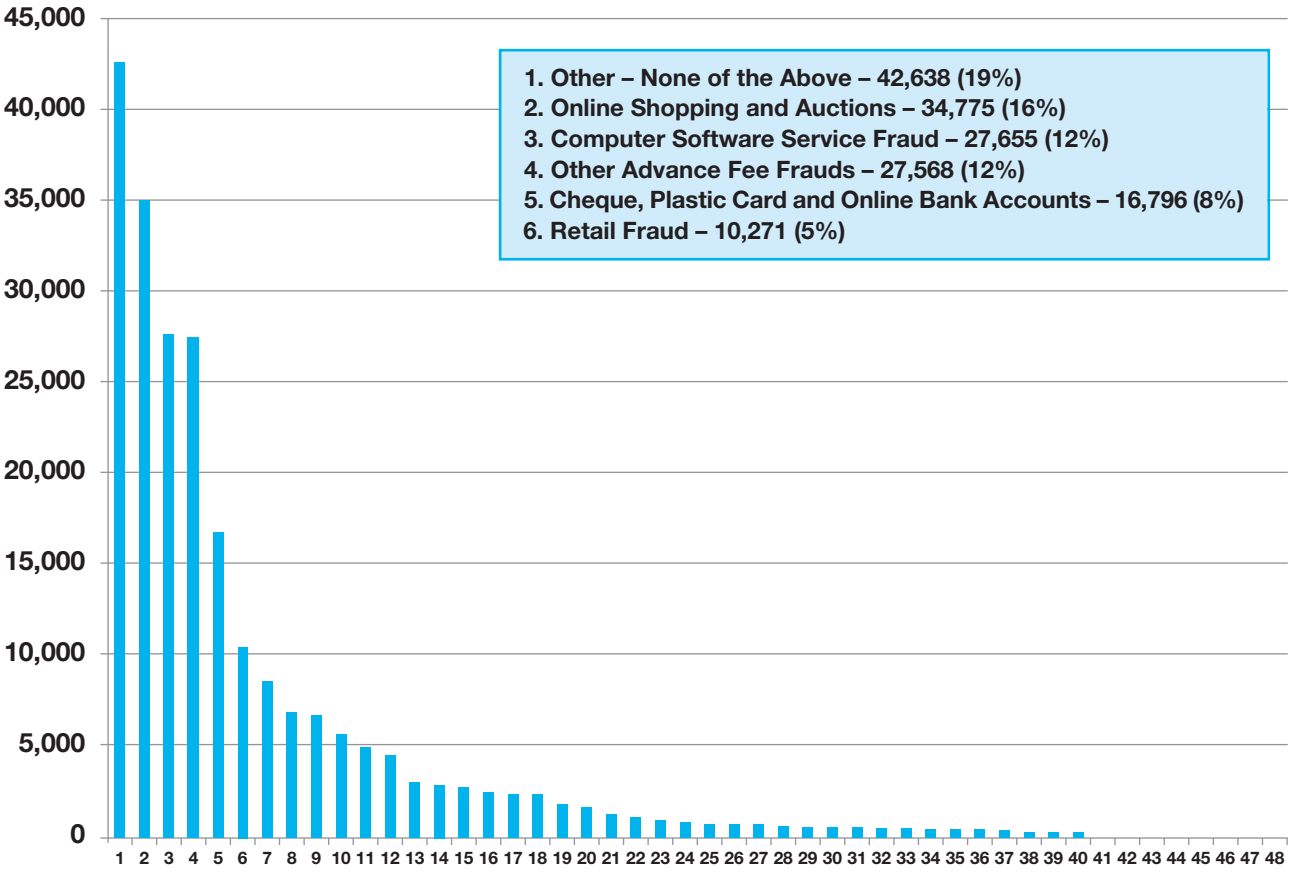
[15] See Appendix C for a breakdown of figures and data reference.

As described above, the police use a total of 48 separate categories (Home Office, 2018a) [16] for fraud but analysis shows crime reports are concentrated in just a small number of them. Figure 3 below shows that just six categories accounted for 71 per cent of all fraud reported in 2016-17. This includes online shopping and auction (16 per cent) and retail frauds (five per cent), two categories that encompass a broad range of fraud offending that occurs within these commercial environments.

Computer Software Service fraud (12 per cent) is also a high volume category in which offenders exploit a specific product or service to defraud victims. Many advance fee frauds are classified as 'other' (12 per cent). Unsurprisingly, some fraud categories relating to specific products or services such as Time Shares and Holiday Clubs (n=180, 0.1 per cent) and Pyramid or Ponzi share schemes (n=58, 0.03 per cent) are reported in very low volumes. [17]

Compared to the vast scale of fraud affecting England and Wales, the police response is very limited (see Figure 4). In 2017-18 while 638,882 frauds were recorded by the police and industry bodies, far fewer crimes (49,861) were allocated an investigation [18] and fewer still (8,313 crimes) resulted in a charge/summons, caution or other positive outcome during that period (Home Office, 2018b). Proportions are difficult to calculate [19] but for nearly every thirteen frauds reported in a single year, one gets allocated for investigation, and for every 77 reported, one reaches a positive criminal justice outcome.

FIGURE 3: A breakdown of frauds reported by local victims in England and Wales in 2016-17.



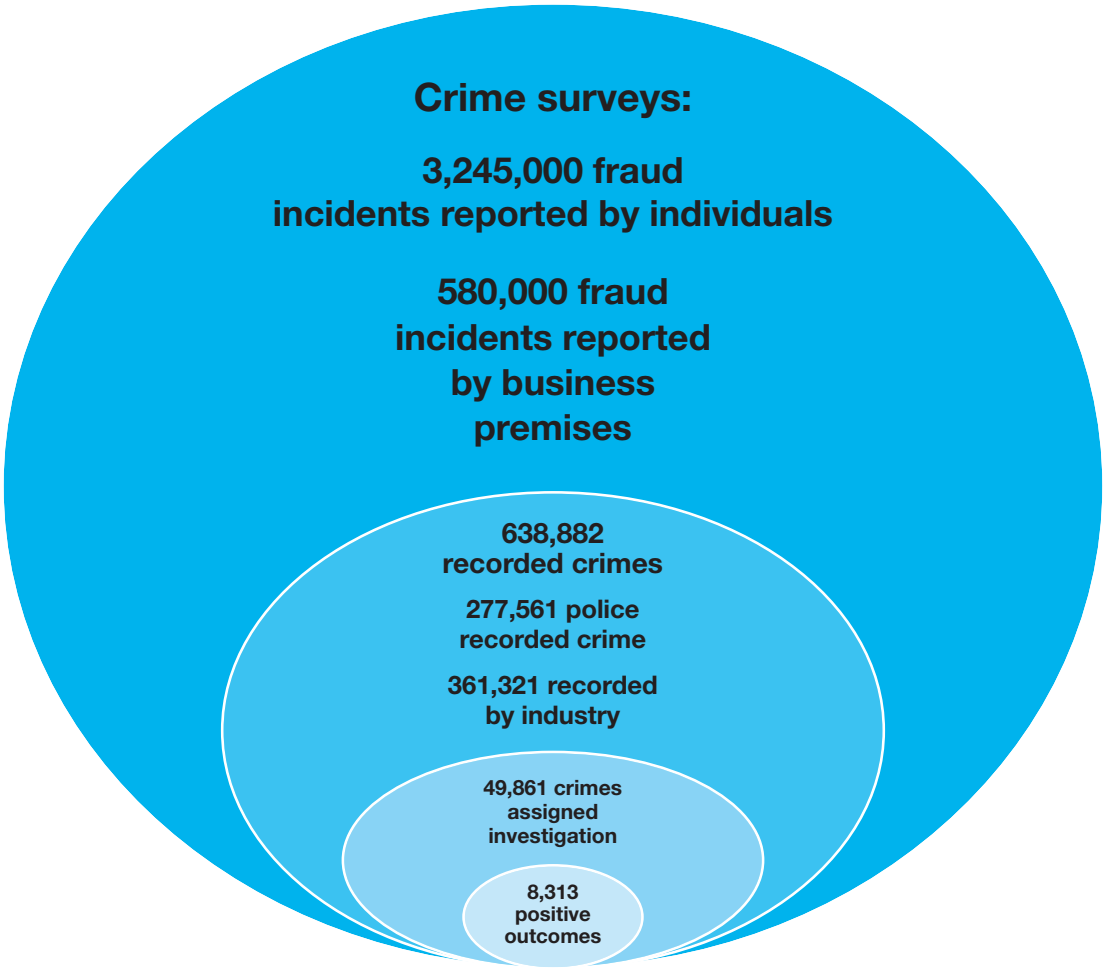
[16] A full breakdown of each offence classification and description is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694449/count-fraud-apr-2018.pdf [accessed 27.09.2018].

[17] It is not in all cases possible to discern whether the variation reflects the distinction between high and low volumes, differential reporting rates by offence category or simply a lack of understanding of the categories by those reporting or recording the crimes.

[18] Multiple crimes may be linked to a single *case* and these crimes pertain to 11,094 cases allocated for a response.

[19] Due to the nature of systems for processing frauds and protracted investigation times, the figures for the number of frauds reported, allocated and then recorded with an outcome are not necessarily crimes drawn from the same reporting period. For example, a recorded charge may pertain to fraud reported in the previous year or earlier and a crime may be allocated at a later date should subsequent intelligence raise new investigative opportunities.

FIGURE 4: The scale of fraud compared to the scale of the response, 2017-18.



Source: Office for National Statistics 2018; Home Office, 2018b; Home Office 2018c.

2.4 THE RELATIONSHIP BETWEEN CYBERCRIME AND FRAUD

Cybercrime is now a major dimension of crime in England and Wales and a major driver of fraud. The government distinguishes cybercrimes by the degree to which they are reliant on the use of Information and Communication Technology (ICT) (HM Government, 2016):

- Cyber-dependent crimes 'are offences that can only be committed by using a computer, computer networks, or other form of ICT'.
- Cyber-enabled crimes 'are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT.

While not recognised in the government's strategy, cyber-assisted crimes are a third category adopted by a report from the City of London Police and defined as crimes that 'use networked digital technologies in the course of criminal activity which would take place anyway' (for a fuller discussion see, Levi et al, 2015; McGuire and Dowling, 2013).

Cyber dependent crime is an essential first step to committing some frauds. For example, the National Crime Agency states that the most sophisticated and serious cyber criminals affecting the UK are deploying malware for defrauding businesses (National Crime Agency, 2016), and the financial sector identifies cyber dependent crime as the primary cause of much of card-not-present and online banking fraud (DCPCU, Unpublished). The amount of data available and the ubiquity of digital identities, such as email addresses and account numbers, present 'rich pickings' for fraudsters who use them to enable volume crimes such as identity and mass-marketing fraud (Button et al, 2014a; Holt, 2013; Sandywell, 2009; McGuire and Dowling, 2013).

Much fraud is ***cyber enabled***. Many such crimes involve establishing direct contact with victims online to defraud them by a process of 'social engineering', a term used interchangeably with 'scamming', to refer to the methods used to trick, deceive or manipulate victims into

giving out personal information or funds [20]. Social engineering is not restricted to the internet, but the internet radically increases the opportunity to draw more people in with minimal effort and risk, and has been central to offences such as dating fraud (Whitty, 2018) and mass-marketing fraud (Button et al, 2014a).

The relationship between fraud and cybercrime is complex as it takes different forms depending on the type of technology adopted, the extent to which it is used and the stage in the offence at which it is employed (Levi et al, 2015). The complexity of the relationship between cybercrime and different types of fraud is illustrated by police investigation case study 1 below taken from one of the case files we examined for this project.

Police investigation case study 1 Money mule

A rental fraud occurred when an overseas student responded to a fake advert for student housing on social media and lost over £1,000. A suspect was identified from the account where the rent deposit was sent. This suspect claimed to have met a female on a dating website who had asked if he would be willing to let others send money to his account and then transfer this to her friends via a money service business.This included transfers to African countries and the identity of these overseas suspects was unknown. The role of the initial suspect (the account holder) in money laundering and whether he himself benefited financially was unclear, with some suspicion he was himself a victim of romance fraud.

How much fraud involves cybercrime?

Cybercrime has considerable influence over the size and shape of the fraud problem, and in turn, the resource and capabilities required to deal with it.

First, we look at what we can understand from recorded crime data. It is difficult to empirically measure the connection between recorded crime and cybercrime, largely because crime recording is not configured to capture contextual factors such as whether the crime occurred online (College of Policing, 2015). Nevertheless, there are indicators in the recorded fraud data which we can use to identify cybercrime:

- Some fraud offences (barring exceptional circumstances) have an inherent online component – these are computer service software, dating and online shopping and auction fraud.
- Sometimes fraudsters use online communications to prompt or initiate contact with the victim.
- Sometimes the manner in which money is taken involves online methods [21].

We used these three indicators to find out how much recorded fraud is cyber-enabled. We took a national sample of cases allocated by the National Fraud Intelligence Bureau for an enforcement response in a single year (2016-17).

We should note at the outset that these data are not without their limitations. First, much of the information is self-reported so dependent on a victim's understanding and recollection of the offence. Second, this sample is not representative of all frauds reported to the police but is restricted to cases that were allocated an enforcement response [22]. Finally, while money sent or taken from bank accounts will encapsulate fraudulent card-not-present payments and crimes in which victims are tricked into transferring money online, it does not exclude identity fraud that involves offline payment methods (for example, use of a fake stolen card in store or over the phone). However, statistics from the not-for-profit organisation Cifas [23] indicate the vast majority (87 per cent) of identity fraud is perpetrated using the internet and for this reason it was used as one of our three indicators of cybercrime.

We looked at 64,857 fraud cases passed on for enforcement action in 2016-17. We found that 69 per cent of cases included at least one indicator of cybercrime. When broken down by the three indicators:

- 27 per cent of cases were fraud offences that were intrinsically identifiable as cyber-enabled.

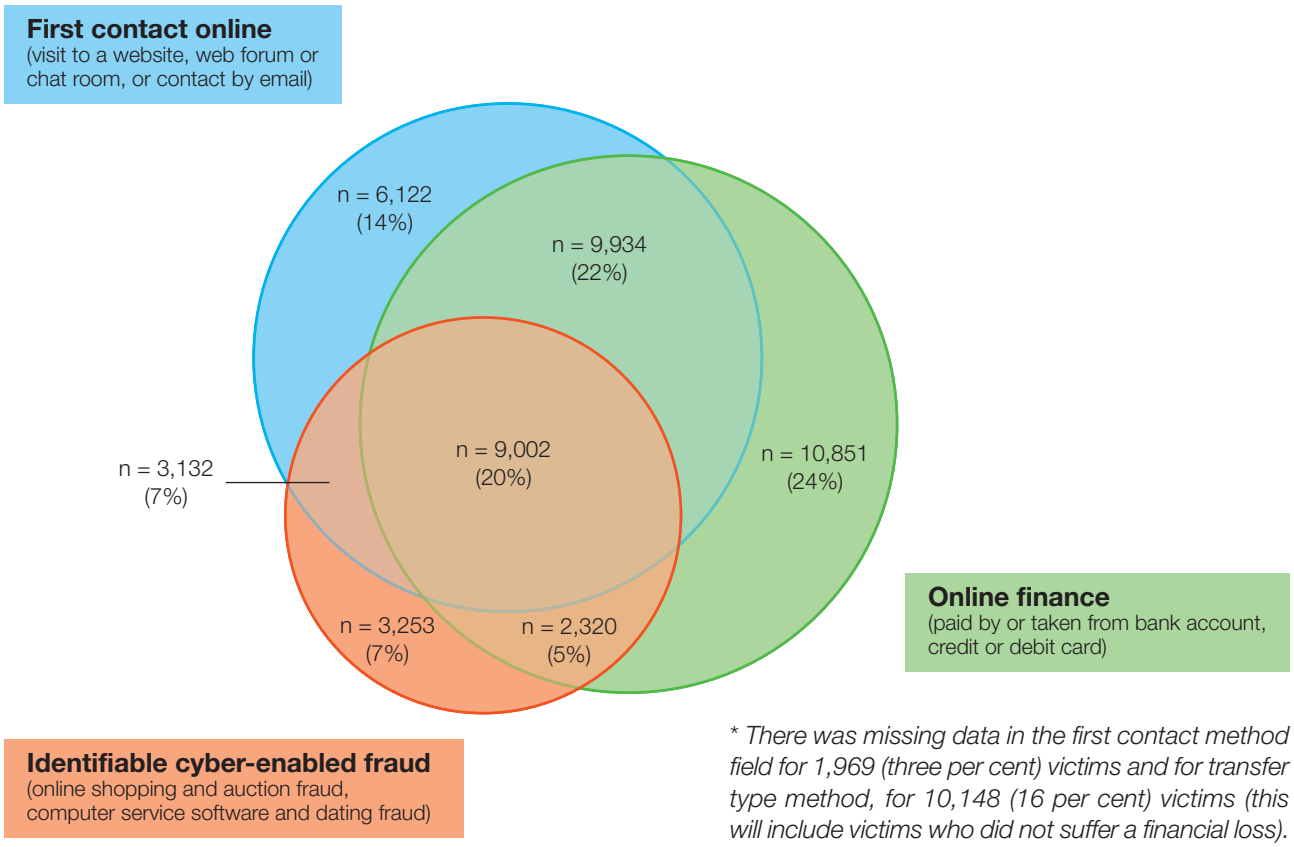
[20] For example, see https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud [accessed 15.08.2018].

[21] The indicator used was 'paid by or taken from credit or debit account, online account'. Other options not included as an indicator were 'paid in cash, cheque or by money transfer'. While the latter can include online financial transfers, the decision was taken to exclude this offence type due to the potential to include victims who used high street outlets. There were 3,048 cases and nearly two-thirds (63.4%, n=3,048) are included in Figure 5 on the basis of being either an identifiable cyber-enabled fraud or where first contact was made online.

[22] Thereby excluding the majority of cases that are not allocated a response. We were unable to access a sufficient sample of frauds reported to the police during this period.

[23] These statistics are taken from a bespoke statistical output provided by industry representative body, Cifas. This analysis reflects the recorded status of each offence on the date that the data was extracted (21/09 /17).

FIGURE 5: The role of cybercrime in frauds allocated for a response in 2016/17.



** There was missing data in the first contact method field for 1,969 (three per cent) victims and for transfer type method, for 10,148 (16 per cent) victims (this will include victims who did not suffer a financial loss).*

- 43 per cent were cases in which the first contact method was online.
- 49 per cent involved money being sent or taken from an account.

Figure 5 shows a considerable overlap between these three elements of cyber fraud, with one in five offences possessing all three indicators. It shows that for the fraud types with an inherent link to cybercrime a great many of them involved contact that was initiated online and/or payments taken directly from the victims' accounts. For the minority of such cyber enabled offences where this was not the case, most pertained to Computer Software Service fraud[24]; a fraud in which first contact is commonly established by phone before a victim is tricked into giving a suspect remote access to a computer.

We went on to break down this sample into different categories of fraud and here we can see that the involvement of cybercrime varies considerably by fraud type:

- Some types of fraud almost always involve cybercrime, including mandate fraud (94 per cent), ticket fraud (95 per cent) and rental fraud (89 per cent) which all included at least one indicator of cybercrime.
- Online contact was not a significant element in some types of fraud such as cheque, plastic card and online bank account fraud (19 per cent). In these cases offenders commonly use fake or stolen details without the need for direct contact with individual account holders (for example, card-not-present fraud).
- Sending or having payment taken from an account was a significant element of the modus operandi for frauds such as lender loan or other financial investment fraud, but contact was more commonly initiated by phone (69 per cent and 42 per cent respectively).
- The role and the significance of the internet varies for different types of fraud: [25] for example, frauds involving door-to-door salespeople are perpetrated in person, but a high proportion of victims reported money being sent or taken from their account (60.5 per cent). In contrast, mandate fraud is shown to be an offence commonly perpetrated remotely with three quarters of cases (75 per cent) involving first contact being established online and a high proportion involving payments being taken or sent from the victim's account (80 per cent). [26]

[24] For these crimes with no link with the other cybercrime indicators 75.8% (n=2,465) were Computer Service Software frauds.
[25] To some extent reflecting the distinctions that have been drawn between cyber-assisted and cyber-enabled crimes.
[26] See Appendix C for a break-down of all fraud categories.

TABLE 3: Fraud categories with the highest volumes of cases with a cyber indicator, 2016-17.

	At least one cyber indicator	First contact online	Payment taken or sent from account	Total recorded fraud 2016-17
Other Fraud	4,580 (62%)	2,931 (40%)	3,164 (43%)	7,365
Mandate Fraud	3,550 (94%)	2,843 (75%)	3,011 (80%)	3,774
Other Advance Fee Frauds	2,912 (46%)	1,837 (29%)	2,086 (33%)	6,277
Ticket Fraud	2,905 (95%)	2,168 (71%)	2,572 (84%)	3,061
Cheque, Plastic Card and Online Bank Accounts (not PSP)	2,152 (54%)	767 (19%)	1,697 (43%)	3,955
Other Consumer Non Investment Fraud	2,151 (82%)	1,201 (46%)	1,868 (71%)	2,634
Lender Loan Fraud	1,750 (69%)	669 (26%)	1,434 (56%)	2,542
Rental Fraud	1,173 (89%)	923 (70%)	943 (72%)	1,312
Other Financial Investment	1,041 (64%)	406 (25%)	886 (54%)	1,636
Application Fraud (excluding Mortgages)	718 (53%)	604 (44%)	147 (11%)	1,366

* This table excludes online shopping and auction, computer service software and dating fraud because these categories were assumed in the analysis to be cyber-enabled.

The categories of fraud where the internet was not a significant factor included some that were targeted directly at businesses or the government. For example, Figure 6 shows that only a minority of retail frauds have a cyber-element (eight per cent). It is however significant that of the fraud categories occurring in the highest volumes in this sample, many show considerable overlap with cybercrime (see Figure 6 below). For example, fraud using online shopping and auction sites comprises one in five (21 per cent) of all frauds which were allocated an enforcement response in this period.

FIGURE 6: Volume of cybercrime indicators in the top ten highest volume fraud categories.

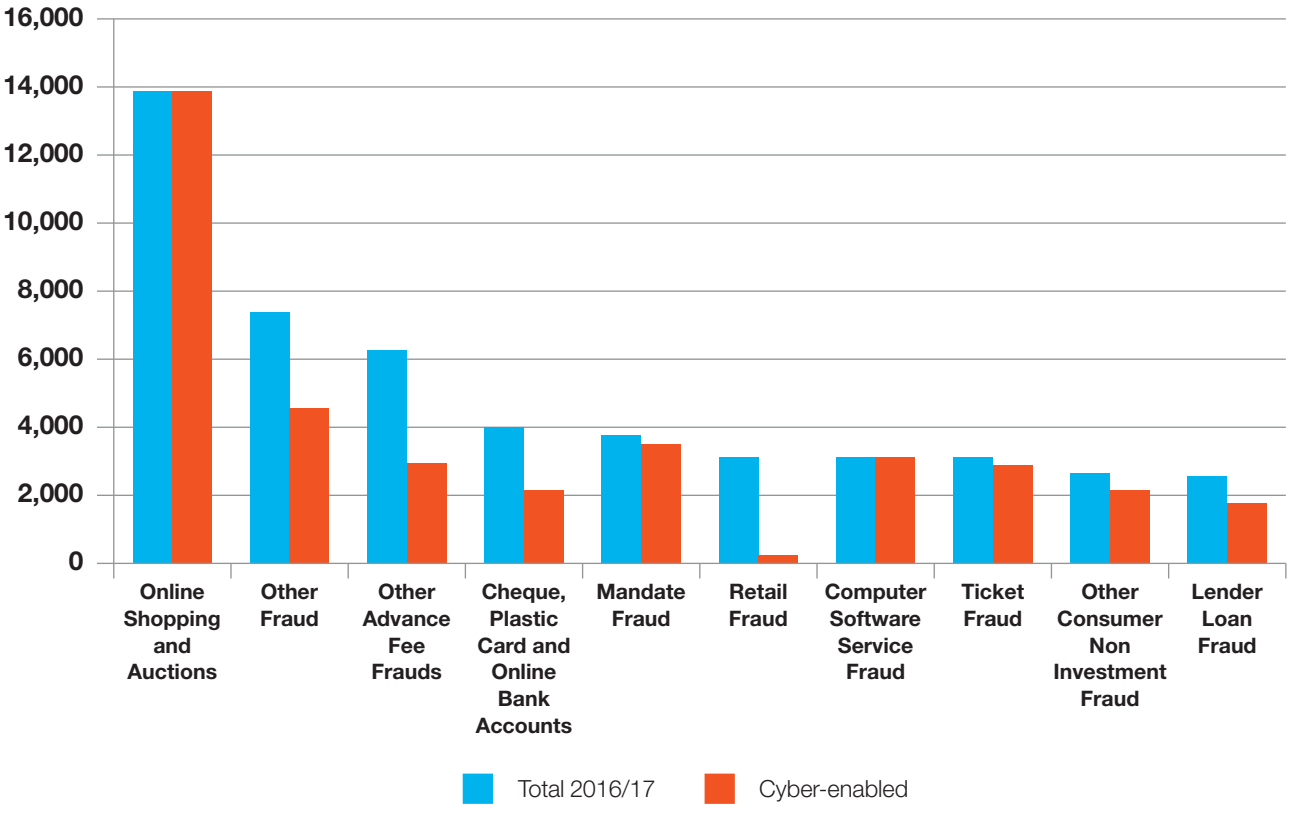
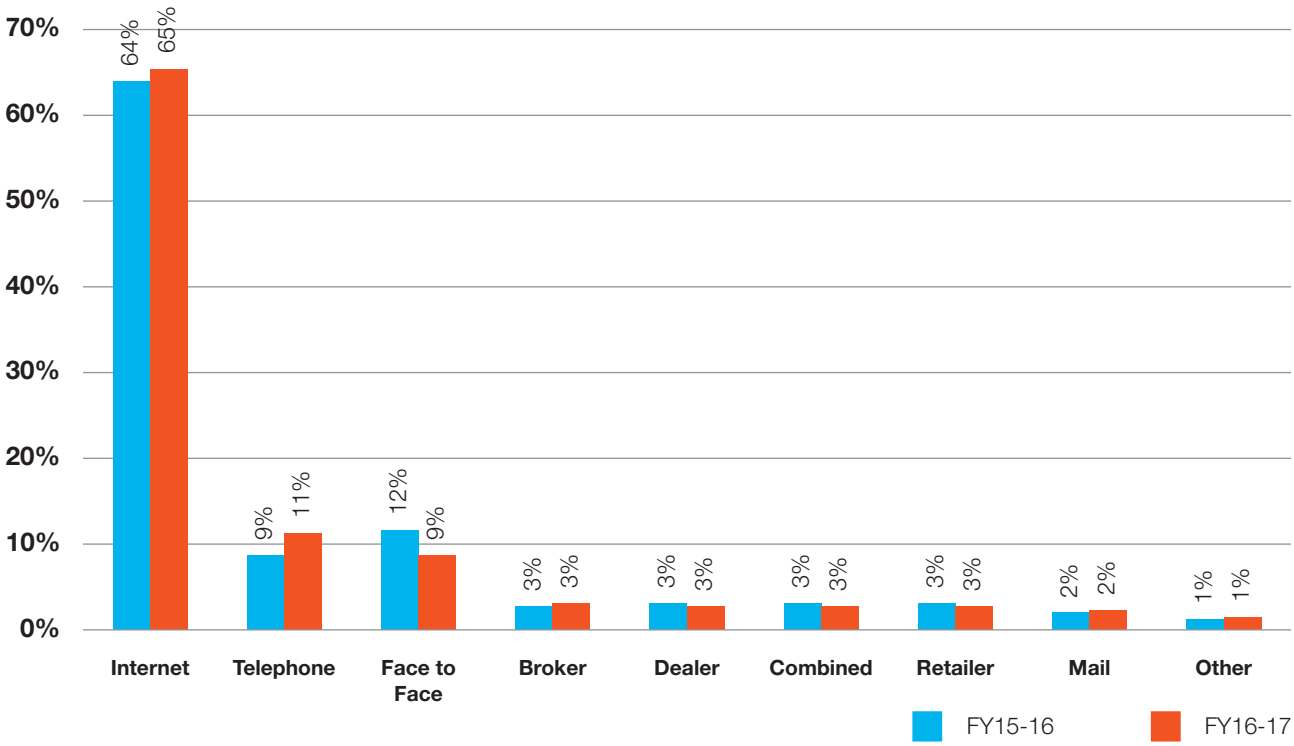


FIGURE 7: Enablers of fraud recorded by industry representative body, Cifas.



Another source for understanding the connection between fraud and cybercrime is the Crime Survey for England and Wales (CSEW), which provides a perspective on all fraud including fraud that is not reported to the authorities. In the CSEW for the year ending March 2018, 54 per cent of fraud is classified as having a link to cybercrime, defined as fraud in which the internet or any online activity were involved in any aspect of the offence [27].

In the CSEW, frauds that used bank or credit accounts linked to the victims were by far the most prevalent type of fraud experienced (69 per cent) and 44 per cent of this category is classified as cybercrime.

A lot of fraud is recorded by the business sector (especially financial services). From data provided by Cifas, nearly two-thirds (65 per cent) of over 320,000 [28] frauds in 2016-17 were perpetrated using the internet [29] (see Figure 7 above). The vast majority is comprised of identity fraud [30] which makes up 65 per cent of all fraud recorded by industry and was predominantly perpetrated using the internet (87 per cent).

2.5 FRAUD AS A CROSS BORDER CRIME

How much fraud involves remote offending? Looking at frauds allocated for a police response in 2016-17, 78 per cent involved a victim and a suspect who did not live in the same police force area [31]. This leaves 22 per cent of frauds allocated for investigation where both the victim and suspect are thought to reside in the same police force. Just four per cent involved overseas victims and three per cent overseas offenders. However this information pertains to crimes not yet investigated and in many cases information on suspects was absent or most likely inferred on the basis of identifiers such as

[27] Data for year ending March 2018 can be found at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables [data accessed 15.08.2018].

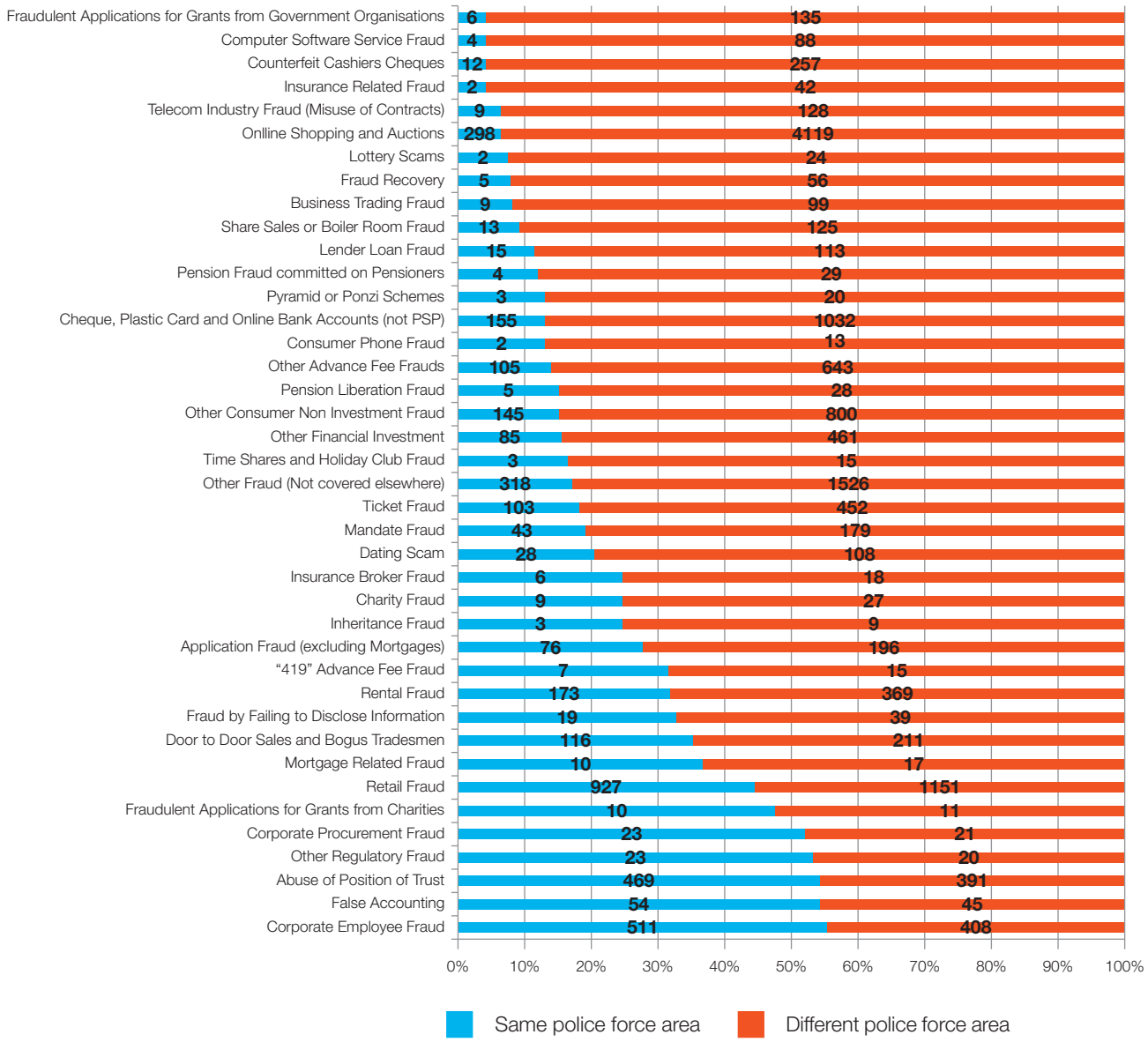
[28] The total number was 324,465. This analysis reflects the recorded status of each offence on the date that the data was extracted [25./06.18].

[29] The definition for fraud that is perpetrated using the internet was simply 'crime with any online component'.

[30] This involves using stolen or false personal data to abuse an account or product. Other categories recorded are Asset Conversion, Application Fraud, False Insurance Claims, Facility Takeover Fraud and Misuse of Facility Fraud. A definition of each category can be found at https://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/External-Fraudscape%20report%202017.pdf [data accessed 08.11.2018]

[31] There was missing data for the locations of many suspects (and to a much lesser extent victim) therefore this data captures analysis of 17,277 crimes. The data represents crimes in which a suspect and their location are known so is unlikely to be representative of all frauds (in particular those perpetrated anonymously).

FIGURE 8: Allocated crimes in which the suspected offender and victim address are in the same police force area, by fraud category (2016/17).



account information. This means that the involvement of offenders operating across national jurisdictions is likely to be substantially underestimated.

Figure 8 shows that the extent of remote versus local fraud offending varies considerably by fraud category. There were ten categories for which a third or more of allocated frauds had an offender and victim located within the same police force area [32]. A high proportion of fraud against businesses such as corporate employee fraud (56 per cent) and retail fraud (45 per cent) show an offender and victim co-located in the same police force. This is also true of offence types that were allocated in high volumes that target individuals, including abuse of position of trust (54.5 per cent) and door to door sales (35 per cent), both of which can include serious financial abuse of vulnerable people. In just under a third of rental frauds the suspected offender and victim address were located within the same police force area.

Notably only four per cent of computer software service and seven per cent of online shopping and auction fraud (two frauds that can be clearly differentiated as cyber-enabled) have a victim and suspected offender address that is co-located. This analysis indicates distinct elements of fraud that have a local dimension and so are potentially more amenable to locally based interventions by the police or partners. [33]

[32] Fraud categories with ten or less cases were excluded from Figure 8. See appendix C for a complete breakdown.

[33] It should be noted that it is highly likely that during the course of an investigation new offenders, addresses and victims may be uncovered which will be missing from this data.

2.6 VICTIMISATION

Fraud victimisation follows a different pattern to victimisation for most crimes (Office for National Statistics, 2016a). According to ONS statistics (ibid.) victimisation is higher in the middle of the age distribution with adults aged 45 to 54 more likely to be victimised than either 16-24 year olds or those aged 75 or over. Fraud victimisation was higher in households with an income of £50,000 or more compared to lower income households. People in managerial and professional occupations were more likely to be victims of fraud than those in routine or manual occupations, full-time students, or those who had never worked or were in long-term unemployment. Additionally, people in rural areas were more likely to be a victim, as were those living in the most affluent areas. In addition to following different victimisation patterns, these statistics challenge popular conceptualisations of fraud victimisation (Deevy et al, 2012), for example, that fraud is a crime that happens largely to older people.

2.7 HARM

The common misconception that fraud is a 'victimless' crime (Button et al, 2014) has been matched by a lack of research and interest in the needs of, and services required by fraud victims. Research into the public's concerns about organised crime (Bullock et al, 2010) has shown that harms from fraud are commonly seen as being absorbed and carried by banks, institutions or society as a whole, rather than by individuals or communities.

Similarly, rather than considering the harm subjectively experienced by victims, much of the research into the impact of fraud has focused almost solely on the financial costs to the public or private sector, or to the wider economy; for example, the National Fraud Authority estimated loss to the UK economy to be £15.5 billion in 2012-13 (National Fraud Authority, 2013).

Recently, however, a body of work has emerged that has begun to demonstrate the breadth of possible impacts fraud can have on a victim. These include financial, social, emotional and physical consequences, which can relate to the victims directly and also to their family and/or their businesses (for example, see Pascoe et al, 2006; Button et al. 2009a) reported on the range of impacts a sample of almost 2000 fraud victims had experienced, and found that it frequently bore little relation to the financial loss experienced. 68 per cent of victims reported strong feelings of anger resulting from fraud, 45 per cent felt that the financial loss had a significant effect on their emotional wellbeing, 44 per cent felt that the fraud had caused stress and 37 per cent reported a significant psychological or emotional impact. A smaller number of victims reported relationship problems, mental or physical health issues or feelings of suicide; some victims reported attempting suicide.

Some impacts are specific to or exacerbated by the nature of fraud. Fraud victims frequently feel ashamed and embarrassed by their victimisation, feeling responsible for it (Cross et al. 2016b) and these feelings created a barrier to accessing both formal and informal support from family and friends. Relationship breakdown, which further isolates a victim, has also been documented as a result of fraud, sometimes partly attributable to loss of shared money (see also, Pascoe et al, 2006).

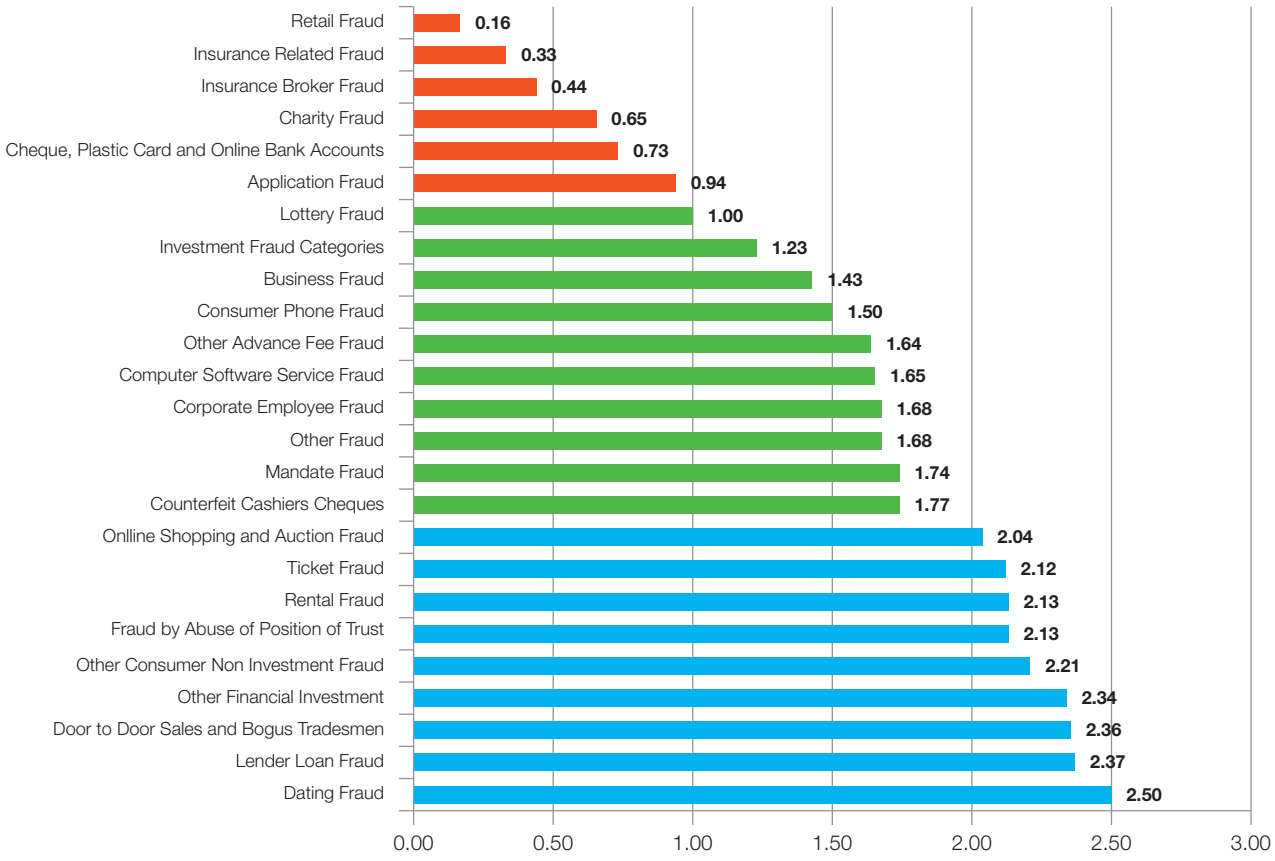
The Fraud Advisory Panel review (2005) highlighted the damaging impact that fraud can have on small businesses. The impacts can include home repossession, jobs and businesses lost, damage and loss of intimate relationships, the consequences of which included physical and mental breakdown, early death and suicide. Small businesses may suffer disproportionate losses from fraud, in comparison to larger organisations that are able to absorb the costs or invest more in fraud prevention. The Federation of Small Businesses (2016) draws attention to the personal impacts of crime against smaller businesses, which are often overlooked:

> *'Crimes against smaller firms are every bit as personal as a crime against a household. A crime against a smaller business should not, as they often are, be seen as impersonal and be seen as attack against an entity rather than a person'.*

It is important to note that certain types of fraud are over-represented in these studies of fraud harm, with a bias towards mass-marketing, boiler room and investment fraud (eg Button et al, 2009a; 2014) and identity fraud (Pascoe et al, 2006). Victims of other types of fraud are either under-represented (such as insurance, ticket or plastic card fraud) or absent from the literature, resulting in a body of research which may not be representative of the experiences of other victims.

We undertook our own analysis of fraud cases allocated by National Fraud Intelligence Bureau for investigation in 2016-17 to understand harm at the individual level (see Figure 9 below). Victims are asked when they report to Action Fraud to self assess the impact they have suffered on a scale, ranging from one to four. In all, seven per cent reported the fraud had had a severe impact on their health or finances and 28 per cent a significant impact. The remainder was split between those who reported being concerned about the fraud (21 per cent) and others for whom the fraud had a minor

FIGURE 9: Average self-reported impact score in cases allocated by the National Fraud Intelligence Bureau for a response, 2016-17. [34]



* All categories with an average impact score of two or more are shaded blue, between one and two green and all under one orange.

impact (18 per cent) [35]. Therefore, contrary to the belief that fraud is a 'victimless' crime, 35 per cent of this sample of victims reported suffering a severe or significant impact, compared to 39 per cent who considered the fraud to be just of concern or having a minor impact.

Figure 9 shows that impact varied considerably by fraud category. On a scale from zero (no response or 'other') to four (severe impact), dating fraud was highlighted as the most impactful with an average self-reported impact score of 2.5. Other frauds with high levels of reported impact were lender loan (2.37), door to door sales and bogus tradesman (2.36) and financial investment fraud (2.34). Frauds with the least impact tended to be those targeting organisations such as insurance related fraud (0.44) and retail fraud (0.16).

Table 4, which shows self-reported vulnerability, reveals an important minority who report being 'vulnerable', with one in five (20 per cent) claiming that they were at risk of losing money, 6.5 per cent that they had been a prior victim and five per cent that they were a regular target of fraud (each victim could answer yes to more than one 'vulnerability'). We should be cautious about these figures because the overwhelming majority of

TABLE 4: Self-reported vulnerability in cases allocated by the National Fraud Intelligence Bureau for a response, 2016-17.

	Risks losing money	Regular target	Prior victim
Yes	12,738 (19.6%)	3,077 (4.7%)	4,192 (6.5%)
No	3,906 (6%)	5,091 (7.8%)	5,580 (8.6%)
No response	48,213 (74.3%)	26,689 (87.4%)	55,085 (84.9%)

[34] A number of police fraud categories were collapsed for Figure 9 and for the following analysis of impact and vulnerability. See Appendix C for a breakdown.

[35] This analysis was out of a total of 64,857 victims, 16,757 (25.8%) either had not recorded a response or answered 'other' – the reasons some have recorded impact in this way is not clear.

FIGURE 10: Correlation analysis of self-assessed impact and vulnerability in cases allocated by the National Fraud Intelligence Bureau for a response in 2016-17, by fraud category. Each bubble represents a different fraud type and the size of each indicates average financial loss.

No.	Fraud category	No.	Fraud category	No.	Fraud category
1	Retail fraud	10	Ticket fraud	19	Fraud by abuse of position of trust
2	Insurance broker fraud	11	Counterfeit cashiers cheques	20	Computer software service fraud
3	Charity fraud	12	Application fraud	21	Consumer phone fraud
4	Insurance related fraud	13	Mandate fraud	22	Other financial investment fraud
5	Corporate employee fraud	14	Online shopping and auction fraud	23	Other fraud
6	Cheque, plastic card and online bank accounts	15	Rental fraud	24	Lender loan fraud
7	Lottery fraud	16	Door to door sales and bogus tradesman	25	Dating fraud
8	Business fraud	17	Other advance fee fraud		
9	Investment fraud categories	18	Other consumer non-investment fraud		

victims had no recorded response and the reason for this is unclear [36].

Our analysis found no association between the levels of financial loss suffered and the recording of vulnerability which may reflect how vulnerability measures in Table 4 focus on *risk* rather than actual harm (or financial loss) experienced. There was also no association between financial loss and self-reported victim impact.

Figure 10, however, shows a strong association between the average self-reported impact score of various 'types' of fraud and the average number of vulnerabilities reported by victims. Fraud categories in the top right of the chart – dating and lender loan fraud (numbers 25 and 24 respectively) – have both the highest average reported impact score and the highest number of vulnerabilities per victim. Other fraud categories with higher impact and vulnerability include other financial investment (22), abuse of position of trust (19), door-to-door sale or bogus trader (16) and other consumer fraud (18). Fraud classified as 'other' also involved victims who experienced higher levels of impact and vulnerability.

[36] By not knowing whether the absence of this data constitutes no response or the absence of vulnerability means it is not possible to know how this affects the composition of vulnerability in the data. Practitioners interviewed commonly highlighted the challenge for acutely vulnerable victims to recognise themselves as such, though in many such cases they would not report the crime.

Fraud types lower on the impact/vulnerability scale were retail (1) and insurance broker fraud (2). This provides a clear differentiation in the self-assessed harm and vulnerability of fraud victims, highlighting segments of victims who might be prioritised for a service from police or others to help them overcome their experience and prevent further victimisation.

Figure 10 also shows the limited association these factors have with financial loss (represented by the size of each fraud category bubble). It is notable that some fraud categories with the highest average loss were those against business; for example application fraud (12) and other business fraud (8). It should be noted that these methods for assessing impact and vulnerability were less applicable to business-related impact or vulnerability. Frauds with the highest average value of losses to individuals included abuse of position of trust (19) (though these frauds can also impact on organisations), investment frauds (9 and 22) and frauds classified as 'other' (23).

What is perhaps most significant about these findings is that they provide evidence to counter the notion that fraud can easily be dismissed as a crime with limited financial, physical or emotional impact on the individual or as a crime for which the most significant impact falls on business or more specifically, the corporate sector (see Button et al 2014; Pascoe et al, 2006; and the victims chapter later in this report). The findings also indicate where much of the harm and vulnerability lies.

2.8 SUMMARY

This chapter has described the nature of the fraud challenge we face as a country. It has defined fraud and shown how it has evolved as a public policy problem over time. Fraud has moved from being a niche white collar crime thought to largely affect business to a volume crime affecting millions of victims each year. Most fraud is unreported, still less is allocated for a police investigation and few investigations result in a positive criminal justice outcome.

Fraud is closely connected with cybercrime and the internet is the primary driver of the increased volumes affecting individual victims. Most fraud is also cross border and hence a challenge to prevent or investigate for practitioners confined to the boundaries of a single police force.

Around a third of fraud allocated for investigation was regarded by its victims has having a severe or significant impact and the data shows that some types of fraud are particularly harmful to victims and tend to target vulnerable people.

3. ENFORCEMENT

Most fraud victims want to get their money back and to see an offender brought to justice (Button et al, 2009b). Yet, as we described in Chapter Two, of the three million fraud offences taking place annually only a small fraction ever end up in court, with the majority either not reported or, if they are, not subsequently allocated a police investigation.

While it is clear that for a complex volume crime like fraud there is no way the police could ever detect most offenders, enforcement against fraudsters remains important. Laws have to be enforced otherwise they lose their meaning and the public will lose confidence in the criminal justice system. A robust enforcement approach is also needed to deter offenders: research shows that increasing the certainty, as opposed to the severity, of punishment, has a deterrent effect on would-be criminals.[37] There is therefore an important moral and practical case for the police to adopt a robust approach to fraud enforcement.

However, fraud investigation is more complex than most other types of criminal investigation and the prospects for successful detections are much lower. This chapter takes a closer look at these challenges and appraises the state of police enforcement in relation to fraud.

In this chapter we do three things. First, we assess the effectiveness of police enforcement activity as measured by traditional criminal justice outcomes. We note that our ability to make judgments about this is hampered by poor data reporting by police forces. Second, we examine the reasons why those outcomes look so poor compared to other types of police investigation. These reasons include the intrinsic complexity of fraud investigation and a deficient system of case allocation, which separates those responsible for understanding the problem (Action Fraud and the National Fraud Intelligence Bureau) from those responsible for investigating it (local police forces). Third, we examine different models for managing fraud investigations at police force level and highlight best practice.

3.1 THE EFFECTIVENESS OF POLICE ENFORCEMENT

Despite being a crime that moves across geographical boundaries our analysis of City of London Police data shows that 92 per cent of the enforcement response in England and Wales is undertaken by local police forces (See Table 5).[38] In what follows we examine how effective those police forces are at investigating fraud and pursuing fraudsters.

The overall effectiveness of police investigations into fraud

Judged by conventional criminal justice outcomes police performance at pursuing fraudsters is poor. The

TABLE 5: The distribution of crimes allocated to the police for enforcement in 2016-17.

	Total crimes	%
England and Wales police force	33,118	92.4%
Other specialist team*	1,304	3.6%
Other police**	1,287	3.6%
NCA-ROCU-National lead force	116	0.3%
TOTAL	**35,825**	**100%**

* Includes the Dedicated Card and Payment Crime Unit and Insurance Fraud Enforcement Department that are partnerships between City of London Police and the private sector.

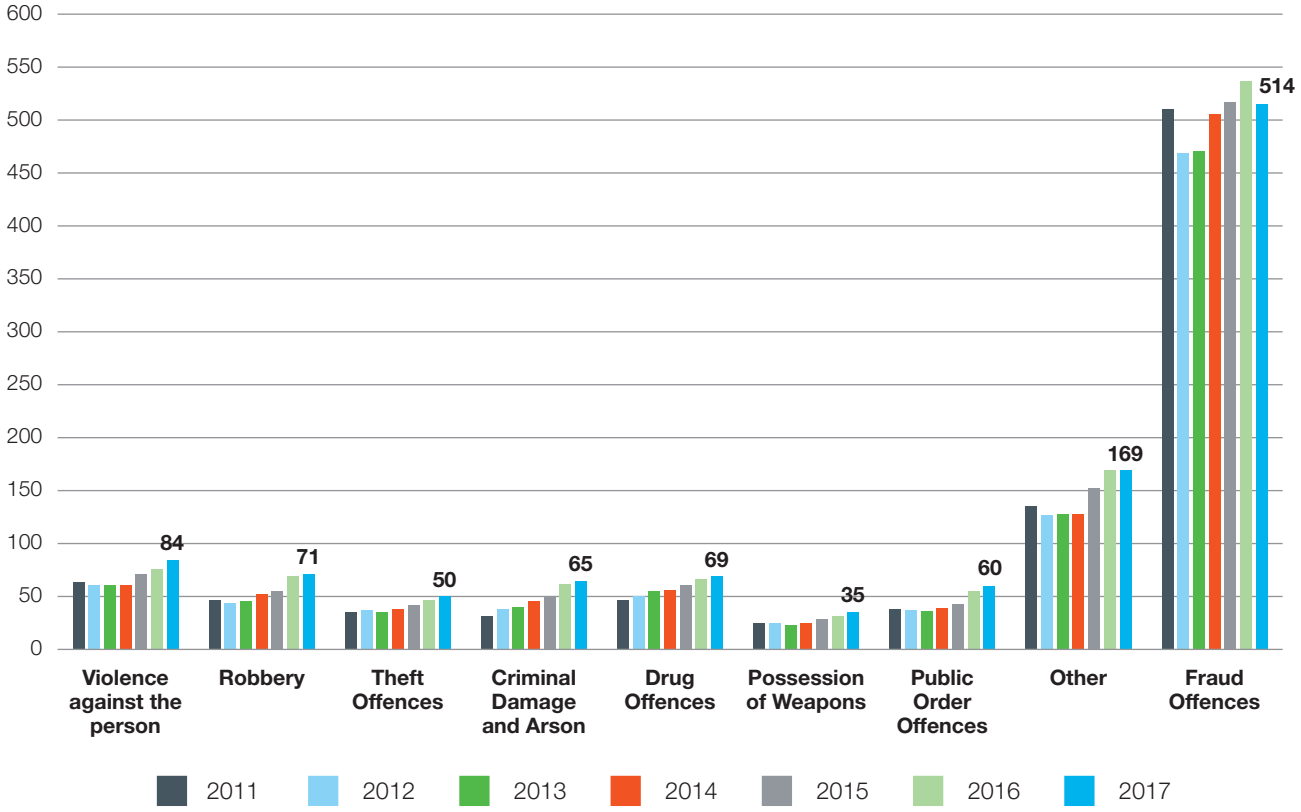
** Incorporates other police forces in the UK

*** There was missing data for the investigating agency in 2,318 cases.

[37] See for example Daniel Nagin and Greg Pogarsky. "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence," *Criminology*, 39(4), 2001.

[38] It should be noted that some of these offences allocated locally could be escalated for a national or regional response at a later stage, (for this to happen the intelligence would need to be developed during the course of the local investigation to demonstrate seriousness or complexity. These onward referrals would not necessarily be reflected in the data although as we will go on to discuss, the indication is that this happens only in a minority of cases).

FIGURE 11: A comparison of the average number of days from the date of offence to charge for fraud and other investigations. [39]



overwhelming majority of frauds do not result in a conviction. While 3.2 million frauds were estimated to have taken place in 2017-18, just 638,882 frauds were recorded by the police and industry bodies. For every crime reported just one in 13 is allocated for investigation and in that same period 8,313 cases resulted in a charge/summons, caution, or community resolution, representing just three per cent of the number reported to the police.

This compares poorly to the percentage of other types of recorded offences resulting in a charge/summons or out of court resolution in the year to March 2018. For example such outcomes were achieved for 15 per cent of violence against the person offences, six per cent of sexual offences, nine per cent of robberies, nine per cent of thefts and 13.5 per cent for all police recorded offences. There is a considerable degree of attrition for most types of crime from the point of reporting to the point of a formal criminal justice outcome, but the outcomes for fraud are worse than for any other type of offence reported by the Home Office. [40]

Fraud investigations also take longer than most other criminal investigations. The average length of time from reporting to charging for fraud offences was 514 days compared to just 50 days for theft offences. [41]

There is, however, some good news. Court data shows the number of convictions for fraud that reaches the criminal courts has gradually increased over the past three years, with for example 1,212 convictions in March 2017 compared to 774 in April 2014 (see Figure 12 below). [42] The conviction rate has been sustained despite the increase in volume.

3.2 POLICE FORCE EFFECTIVENESS COMPARED

What do we know about variation between police forces and law enforcement bodies in the outcomes achieved? The short answer is that it is very difficult to know

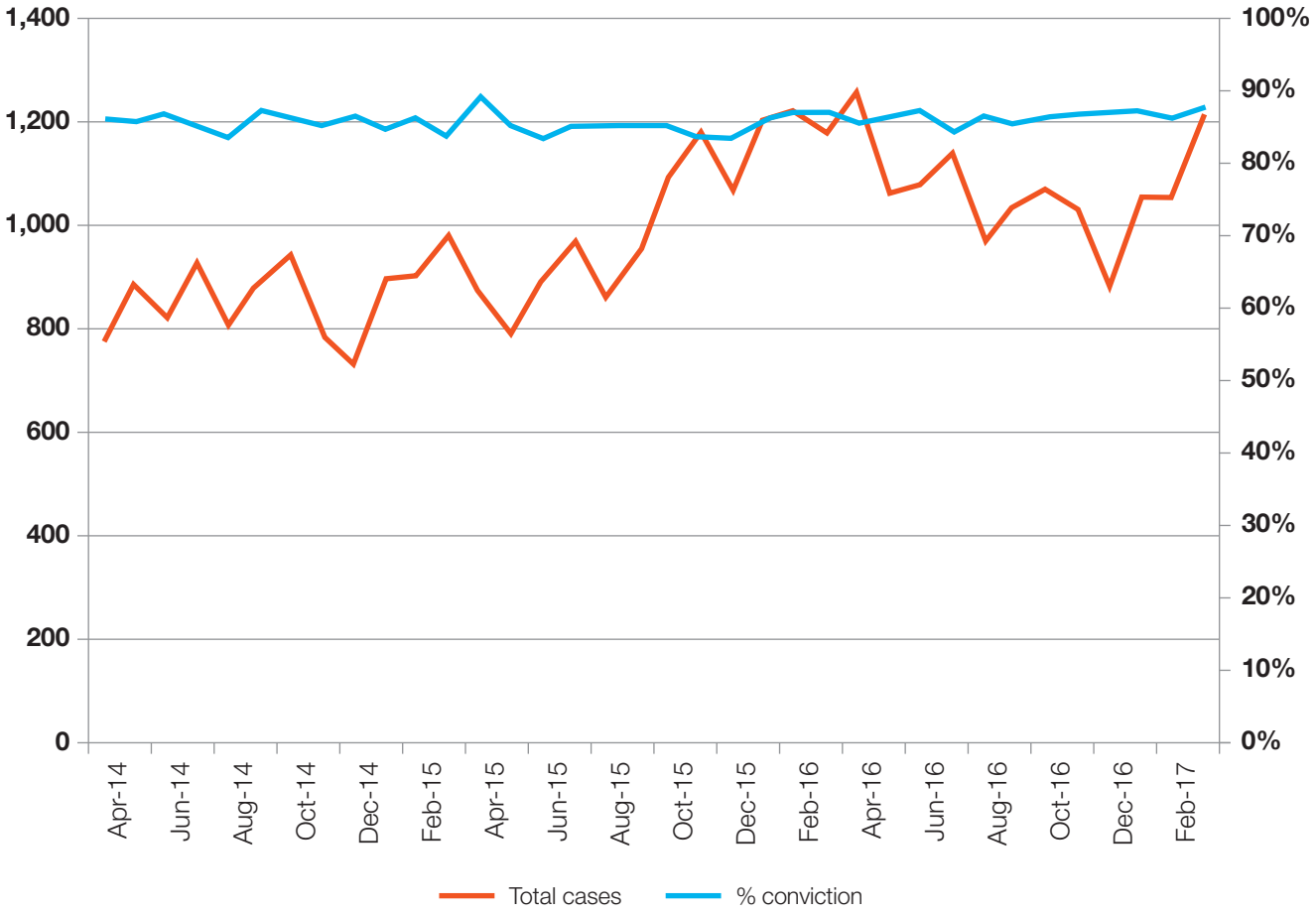
[39] This chart excludes sexual offences where the average number of days from offence to charge was 1,780 days in 2017.

[40] Data sourced from https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2017-to-2018.

[41] Data sourced from https://www.gov.uk/government/statistics/criminal-court-statistics-quarterly-october-to-december-2017.

[42] Data sourced from https://www.cps.gov.uk/publications/performance/case_outcomes/2016_04/index.html. These reports provided a monthly output for the outcomes of Crown Prosecution Service proceedings in magistrates courts and in the Crown Court. Outcomes were broken down into two categories: convictions and unsuccessful outcomes.

FIGURE 12: Crown Prosecution Service cases and outcomes in which fraud and forgery are the principal offence category, April 2014-March 2017.



because of major gaps in the data reported by police forces to the crime recording centre, the National Fraud Intelligence Bureau (NFIB).

Figure 13 below shows the distribution of positive and non-positive outcomes recorded by NFIB (excluding all with no recorded outcome). It shows wide variation by police force however it is likely many are skewed by internal processes. For example, Avon and Somerset recorded only 15 outcomes during this period, over half of which were recorded as positive outcomes. Interviews with local practitioners revealed the vast majority of outcomes were not submitted to the NFIB during this period.

We analysed recorded crimes allocated to local police for enforcement over an 18 month period. This included frauds allocated in April to September 2016 and the outcomes were tracked as far as September 2017[43].

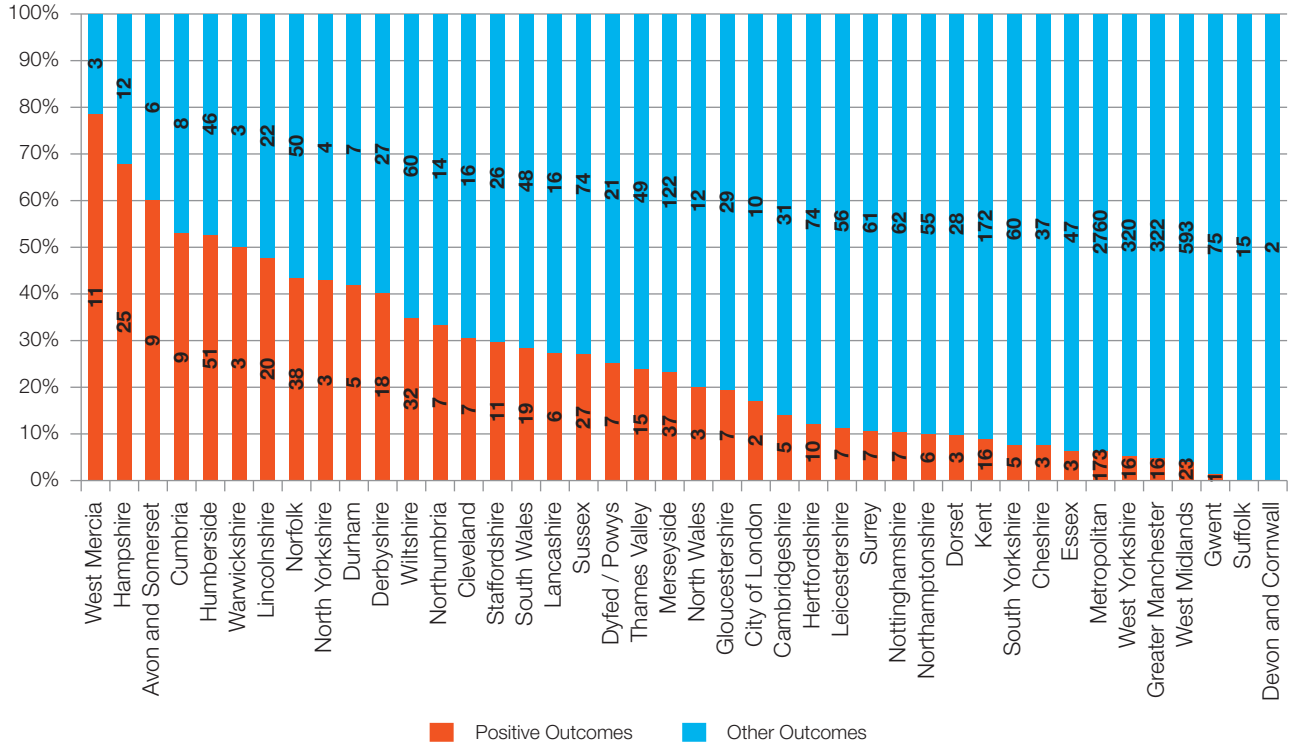
Table 6 shows that:

- 28 per cent of investigations are closed within the first month and few of these led to positive outcomes. The indication is that few fraud investigations are resolved quickly and most likely many that are, are assessed to have no investigative leads and quickly closed following allocation.
- 42 per cent of investigations recorded with a positive outcome had been open for a period exceeding six months[44]. This to some extent supports the notion that fraud investigations can be protracted, but it is not clear how much this is due to complexity and how much due to procedural delays or a lack of prioritisation.
- 52 per cent of frauds allocated still had no outcome recorded 12 months later. The

[43] The sample included investigations allocated in April to September 2016 but the records for each investigation spanned an additional twelve months to September 2017. Therefore the analysis could examine outcomes over a period ranging from 12 to 18 months depending on what date the investigation was allocated within the initial six month period.

[44] A minority of recorded outcomes were for crimes investigated for longer than a year (n=158, 2 per cent) however investigations longer than a year are likely to be under-represented because the sample was restricted to a time period of a maximum of 18 months.

FIGURE 13: The proportion of cases allocated for investigation from April 2016 to September 2016, with a positive or other outcome recorded by September 2017.



proportion of those that constituted complex ongoing investigations is unclear from this data. Analysis of more complete local crime data in Avon and Somerset and Essex[45] showed only a minority of investigations were open for more than 12 months (nine and seven per cent respectively). If only a minority of investigations persist beyond 12 months the indication is that many outcomes absent from the National Fraud Intelligence Bureau data represent an absence of data rather than ongoing enforcement activity.

Recommendation 1: Those responsible for fraud investigations, including police forces or regional units, should be required to monitor and record the outcomes of fraud investigations in a consistent way, according to a template developed by the National Fraud Intelligence Bureau.

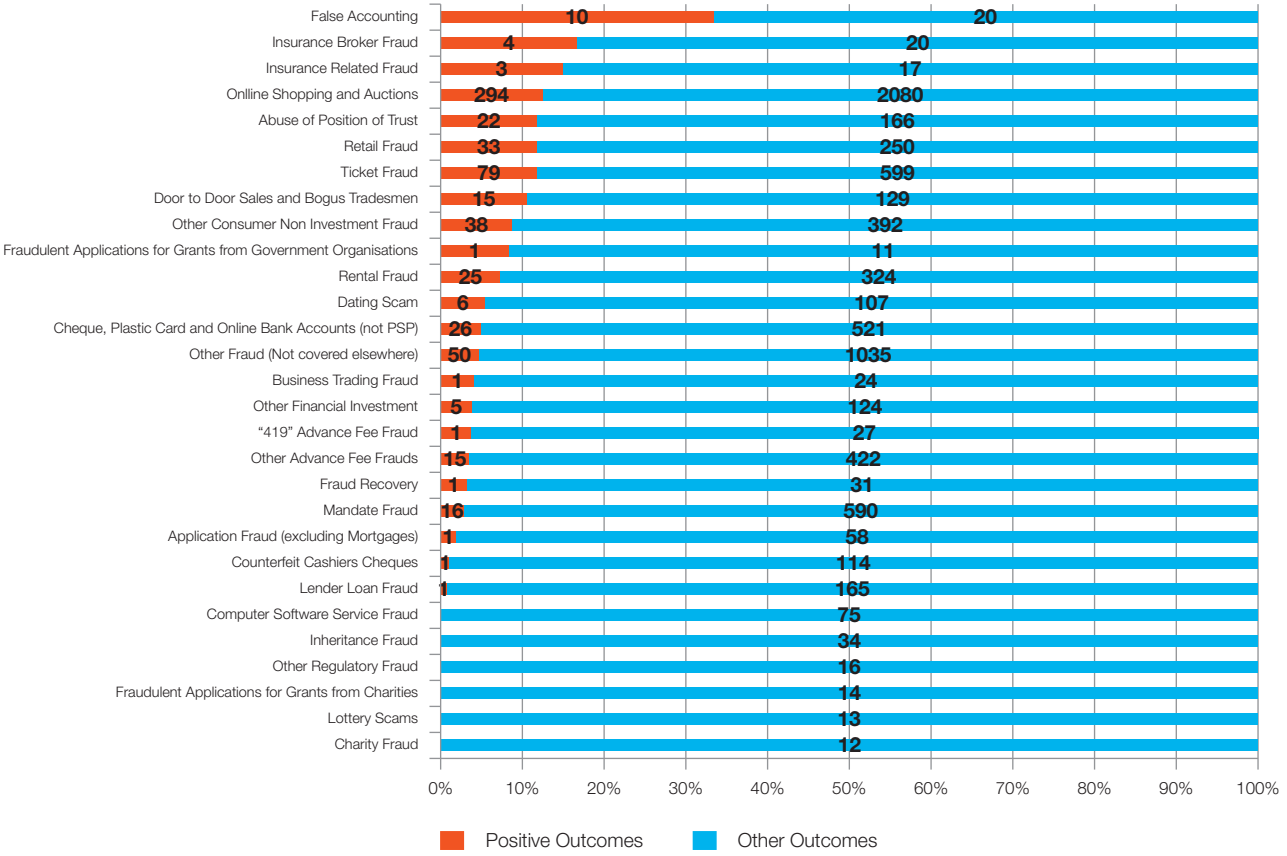
TABLE 6: A comparison in the length of time taken for investigations that lead to a positive or other recorded outcome.

	Positive outcomes		Other outcomes		Total	
Time open	**Count**	**%**	**Count**	**%**	**Count**	**%**
1 week	14	2%	736	10%	750	9%
1 month	56	8%	1,525	20%	1,581	19%
3 months	155	21%	2,012	26%	2,167	26%
6 months	197	27%	1,853	24%	2,050	25%
1 year	284	39%	1,338	18%	1,622	19%
more than 1 year	26	4%	132	2%	158	2%
Grand Total	**732**		**7,596**		**8,328**	

* The reasons for file closure in 'other outcomes' included: filed subject to new information (44 per cent), evidential difficulties (39 per cent), not in the public interest (eight per cent), victim declines to engage or unable to identify a suspect (six per cent) or the investigation was transferred to another body (two per cent).

[45] This sample included frauds that were open or opened within a two year (2015-16 and 2016-17) period by each police force. It was therefore not restricted to frauds allocated only in the two year period nor on case outcomes that are reported back to the National Fraud Intelligence Bureau.

FIGURE 14: A comparison of outcomes by fraud category - crimes allocated for investigation April 2016 to September 2017.[46]



3.3 DIFFERENCES IN OUTCOME BY FRAUD TYPE

Looking at the distribution of outcomes by fraud category reveals some interesting differences. Figure 14 shows that some categories achieved no positive outcomes, such as computer software service and lottery scams. Eight fraud categories culminated in a positive outcome in at least ten per cent of cases, including online shopping and auction fraud, which due to high volumes also constitutes 40 per cent of all positive outcomes recorded in this period.

It is notable that the police achieve more positive outcomes for frauds treated as a 'call for service'. Crimes treated as a call for service are those where the police have chosen to deliver an immediate response. The reasons for doing this can vary depending on local policies but principally they denote frauds perpetrated by an offender physically present at the time of the offence (and therefore more conventionally 'local'). For example, a third (37 per cent) of frauds perpetrated by an employee and a quarter (25 per cent) perpetrated by a professional, relative or associate who abuses a position of trust were classified as a call for service, compared to two per cent of dating fraud and three per cent of computer service software fraud (both of which are predominantly cyber-enabled) [47].

Table 7 shows over a third (34 per cent) of frauds treated as a call for service within the six month period were

TABLE 7: A comparison in recorded outcomes for crimes responded to as a call for service and all other crimes recorded in April 2016 to September 2017.

Disseminated for	Positive outcomes		Other outcomes		Total Count
	Count	%	Count	%	
Enforcement	631	86%	7,403	97%	8,034
Enforcement – Call for Service	101	14%	193	3%	294
Grand Total	**732**		**7,596**		**8,328**

[46] Offence categories with ten or fewer recorded outcomes were excluded.

[47] This illustration is taken from all frauds allocated to the police for enforcement over 12 months.

recorded with a positive outcome, compared to just eight per cent of other frauds. Frauds treated as a call for service comprise 14 per cent of all positive outcomes from this period. This highlights the importance of early identification of opportunities where the prospects for enforcement are high. We discuss this issue of how forces handle a 'call for service' more fully in Chapter 4.

Disruption activity

Disruption tactics are a mainstay for police units tackling serious and organised crime, and represent a variety of means by which to obstruct a perpetrator's offending, contributing to the overall aim of crime and harm reduction. They can also accompany the pursuit of a criminal justice response while delivering a more direct and timely intervention against an offender.

The consideration and adoption of disruption tactics in the course of investigation is less often the norm for generalist investigators but is considered necessary by the City of London Police in the case of fraud. There is a balance to be struck between harm reduction and the pursuit of criminal justice and the City of London Police have developed the Fraud Investigation Model (FIM), which seeks to address this by bringing consideration of disruption tactics into an earlier stage of an investigation (Betts, 2017), especially in light of the protracted and precarious nature of fraud investigations.

Rather than being offender-focused, as might be the case for conventional crime, disruption of fraud offending often involves tackling technological, financial or communication enablers in order to prevent other members of the public being exposed to potential victimisation. Much of the allocated response from the City of London Police is for disruption by in-house teams, principally to arrange the removal of various types of account known to facilitate fraud. This requires extensive engagement with national and international corporations such as web domain providers, banks and telecommunications providers who take the eventual decision to act. The success of these engagements can depend on relationships with the police and the policies and processes of each operator, which assess how 'well-founded' each allegation is (Hutchings, Clayton and Anderson, 2016). Practitioners described more challenges in engaging with businesses in overseas jurisdictions.

The City of London Police estimated telephone, email, website and bank account disruption requests to the private industry saved £360 million in 2016-17. The impact on offending is uncertain, in terms of the extent to which a fraudster is impeded or simply displaced (for example to another online space). Therefore short-term gains need to assessed alongside their long-term value in disrupting an offender but the evidence in this space is thin (Hutchings, Clayton and Anderson, 2016; Levi et al., 2015).

The extent to which 'rank and file' investigators' are conscious of disruption tactics as a viable response option seems questionable, with a number of practitioners indicating that this national disruption team were not well known outside of specialist units in the police.

3.4 THE CHALLENGES OF FRAUD ENFORCEMENT

In the previous section we looked at the outcomes the police achieve in fraud investigations and in what follows we examine some of the reasons why these outcomes are relatively poor compared to other areas of police investigation. We focus on two areas of challenge:

- The intrinsic complexity of fraud as an area of criminal investigation;
- The process for allocating cases for investigation which contains a number of flaws.

The complexity of fraud investigation

Below we outline why fraud is such a complex area of investigation. We focus on three themes that emerged from both our analysis of 25 investigation case files [48] and qualitative input from practitioners in interviews and the survey.

Locating the suspect

Investigations are primarily assigned on the basis of the location of the offender which is commonly inferred on the basis of digital identifiers rather than confirmed identities (especially in the case of online and telephone-enabled fraud). In 15 out of 25 case files we examined, the only geographic identifier for the suspect

[48] This was a purposive sample of cases to cover a range in types of fraud and investigation. See Appendix A for a description of the methodology.

was a financial account, an email or other web account or a phone number, all of which can be manipulated by fraudsters to enable their offending and evade detection.

A number of enquiries led to accounts 'hijacked' by fraudsters to launder funds, suspected money mules or accounts opened with false identities. They could also lead to multiple suspects operating across national or international jurisdictions. Suspects could readily move across locations or switch to new accounts details, especially with the time-lag between the offence and subsequent investigation.

Consequently, many investigations in the case file analysis either failed to uncover a suspect or revealed that the suspect was not in fact local, which curtails the ability of a local police force to develop intelligence and effectively investigate.

Police investigation Case Study 2 Tracking down the suspect

Two victims had given advance payment for high value goods (worth several thousand pounds) advertised on a popular online auction website, which were not delivered. This was reported to have been done by 'spoofing' (or creating a site disguised as) a legitimate payment website. The investigation was allocated to a police force on the basis of the account details of the suspect leading to details registered in a city in the area, and was passed to a local investigation team. After two and a half months, enquiries with the bank revealed multiple linked accounts opened fraudulently using fake identity documents from overseas. All appeared to be linked to the same individual opening accounts across the UK in quick succession. Investigators had little proof of a local suspect but evidence of a network of offenders operating across the UK. The local investigator tried to pass the case over to the Regional Organised Crime Unit (no additional information was recorded to indicate the outcome).

Evidence-gathering

The process of gathering evidence in fraud investigation is conducted more through desk based enquiries than local or physical evidence-gathering. Key information includes details of registered users, transaction details and statements from victims. There are a wide range of organisations officers need to engage with to progress investigations, including other police forces, officials in foreign jurisdictions, banks, web companies and others besides.

The protocols for accessing the required information are varied and bureaucratic. Applications for information are not guaranteed to receive a response and could eventually get declined (in some cases even by other police forces). In addition to being in control of potential evidence these third party organisations can have exclusive understanding of the offence and where lines of enquiry may be, leaving police investigators with limited influence over how an investigation progresses. One local investigator described frustrations in dealing with these third parties:

> *'When those communications data providers are based overseas, getting results from them is nigh on impossible.'*

These enquiries can cause considerable delay. To illustrate, one case file we examined was open for a year while waiting for correspondence from overseas authorities. The degree to which an organisation engages could influence decisions on whether to proceed with the investigation. This undoubtedly contributes to the protracted length of fraud investigations.

Police investigation Case Study 3 Securing evidence

A local business had its telephone system hacked and calls were made to a premium rate overseas phone number which cost them several thousand pounds. The phone service provider was not local and had been linked to an earlier offence against a customer; they had previously declined to assist with the investigation. The phone service provider was emailed to ask if they could identify who had accessed each phone system. Instead of offering assistance they emailed a response which gave a technical description of how the cyber-dependent crime was likely to have been perpetrated and stated it was a result of weak security implemented by the victim. The police decided not to proceed with the investigation.

The challenges of victim management

Victims linked to the case files analysed were geographically dispersed and showed variable levels of engagement with the investigation process. They were uncertain over what they wanted, whether they were a victim of a crime, someone in need of protection or one half of a civil dispute (or indeed all three).

There were multiple examples in the case files of delayed responses or victims failing to respond to investigators contact at all. The reason was not always clear although

it was indicated that reimbursement rather than criminal justice was the primary objective for some, as described by a local police officer dealing with volume fraud cases:

> *'Once the bank have said they can have their money back, they're [the victims are] not really interested in an investigation anymore.'*

However, long delays in investigation could also result in victims becoming less engaged. In one case a small business eventually elected to pursue civil proceedings.This was a point made by a local investigator:

> *'All of this has taken so long that the victim has stopped emailing me and he won't now give a statement.'*

A small number of case files involved fraud perpetrated against victims living overseas and so communication and evidence-gathering was restricted to an email exchange. In one cyber-enabled fraud the investigator had trouble identifying who the victim was from the limited exchange with an overseas company. In another it transpired the individual had not been defrauded of any money but was vulnerable and had been tricked into facilitating money laundering by fraudsters overseas.

Police investigation Case Study 4 Complexities in dealing with victims

A care home administrator reported that an elderly victim's account was depleted by tens of thousands of pounds over time with consequences for the victim's ability to pay fees. The suspect was a family member granted access to accounts due to the victim's health difficulties. The victim had gifted some money however the suspect claimed all the money was taken with consent. The victim disputed this account of events but was more concerned with maintaining the relationship, especially due to poor health and the knowledge that it was unlikely the money would be retrieved. Investigators thought it unlikely the victim would want to proceed with an investigation and eight months later got agreement from the victim for the investigation to be closed.

The process for allocating frauds for investigation

A second reason for the poor outcomes identified above, beyond the intrinsic complexity of investigating fraud, is the process of allocating cases for investigation. Fraud and cybercrime are unique in policing with the decision-making around when to investigate and where to allocate investigations, falling primarily to a national unit (the National Fraud Intelligence Bureau). Most fraud is perpetrated remotely (ie, across force borders), which for locally bounded police forces is a barrier to establishing a clear intelligence picture and delivering an effective enforcement response. A national perspective is required in order to draw together information from victims across different jurisdictions and to coordinate cases so they are allocated to those in a position to investigate. However, we have identified a number of challenges with the process of case allocation, which we explore below.

Data quality

Decision-making is contingent on the quality of information provided by victims via Action Fraud but there are significant gaps in this information.

The City of London Police, through Action Fraud and the National Fraud Intelligence Bureau, records and processes a vast amount of crime data and information reported by individuals and businesses [49]. Its role is to collate and develop cases on the basis of the information provided in these reports, not to develop new intelligence. Therefore the quality of this analysis is contingent on the quality of the information collected from victims.

Previous research has identified problems at this stage as a key contributor to the high attrition rate in fraud investigations, with the majority of recorded crimes failing to incorporate the information needed to make an investigation viable (Scholes, 2018). Our previous research identified that from a sample of recorded fraud nearly a third (32 per cent) had not included any information on offenders (for example, online or bank account details), thereby limiting the prospects that the information could be developed and the case investigated (Crocker et al, 2017).

The system only works when the information that is fed in can be analysed to draw links and identify potential suspects. The absence of relevant information may reflect the degree to which a fraudster's methods remain hidden to the victim, but also the challenges in eliciting the right information in the context of complex victim and crime narratives, especially given the high volumes reported autonomously by victims online. This had been recognised as a problem and at the time of the research, City of London Police was improving the online interface to increase the likelihood that victims provide more relevant information.

Recommendation 2: There should be a review of all fraud data collected and analysed by the National Fraud Intelligence Bureau with the aim of improving the assessment and allocation of crimes

[49] These include relevant information reported by the public that does not include recordable crime.

for investigation. In particular the review should aim to improve the quality of the information provided by victims to Action Fraud.

Case ownership

There is a lack of clarity around who is responsible for a fraud investigation. The national system for processing cases, while necessary for providing a more strategic picture and a more rational process for allocating cases, means that fraud cases pass through many hands before they reach an investigator on the ground. Professional ownership of a case may be diluted as a result. The work done to progress cases at the different tiers of response is driven by different criteria and thresholds.This is inefficient because the time and resource put into developing an investigation can have little or no bearing on how or whether it is progressed at the next stage of allocation.

Since the establishment of Action Fraud there has also been some confusion within the police workforce about its role and responsibilities. Some police officers assume that Action Fraud not only owns the crime, but also the problem and the response, failing to recognise that it has no operational or investigative function; it is simply a crime-reporting hub. One local constable told us:

> *'When Action Fraud came in, no-one knew what they did and they were meant to take all fraud reports and be a central investigation but it's not actually worked out like that as far as I'm aware. They collect it all and it just comes back to us. I don't really get what their [role is], apart from collecting [data] for the government, I don't really know what else they do'*

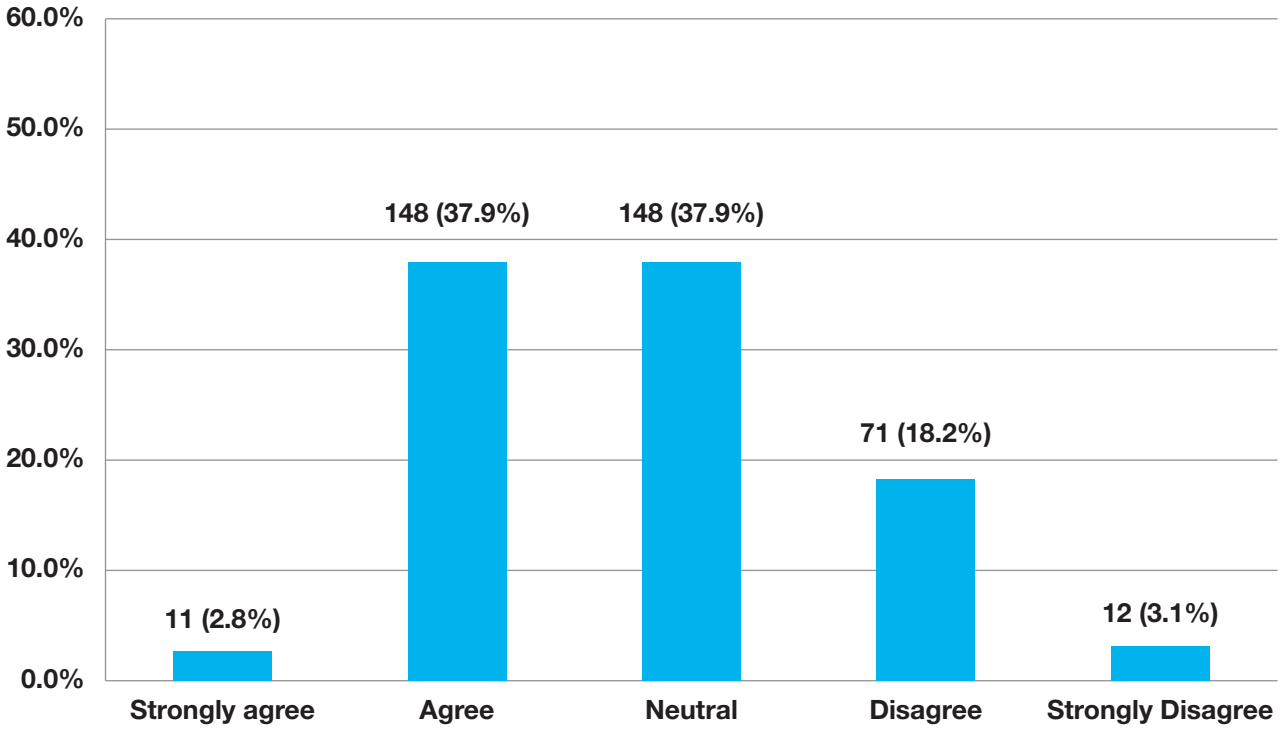
We return to the implications of this problem in Chapter Six below.

Local priorities

The decisions of the National Fraud Intelligence Bureau are detached from the considerations of police practitioners on the ground, working to distinct local priorities and pressures. The City of London Police assign an investigation almost solely[50] on the basis of whether one is viable. However the local police must weigh this up against all other demands, principally on the basis of a perceived view of the threat, harm and risk to victims and others.

As will be described in Chapter Six, fraud is not prioritised strategically at the local level, neither in police and crime plans nor at an operational level by senior leadership teams. Figure 15 below shows in our workforce survey[51] just 39 per cent of officers and police staff agreed that fraud should be a priority in their police force; the increasing volumes and fraud involving vulnerability was highlighted by many practitioners as important.

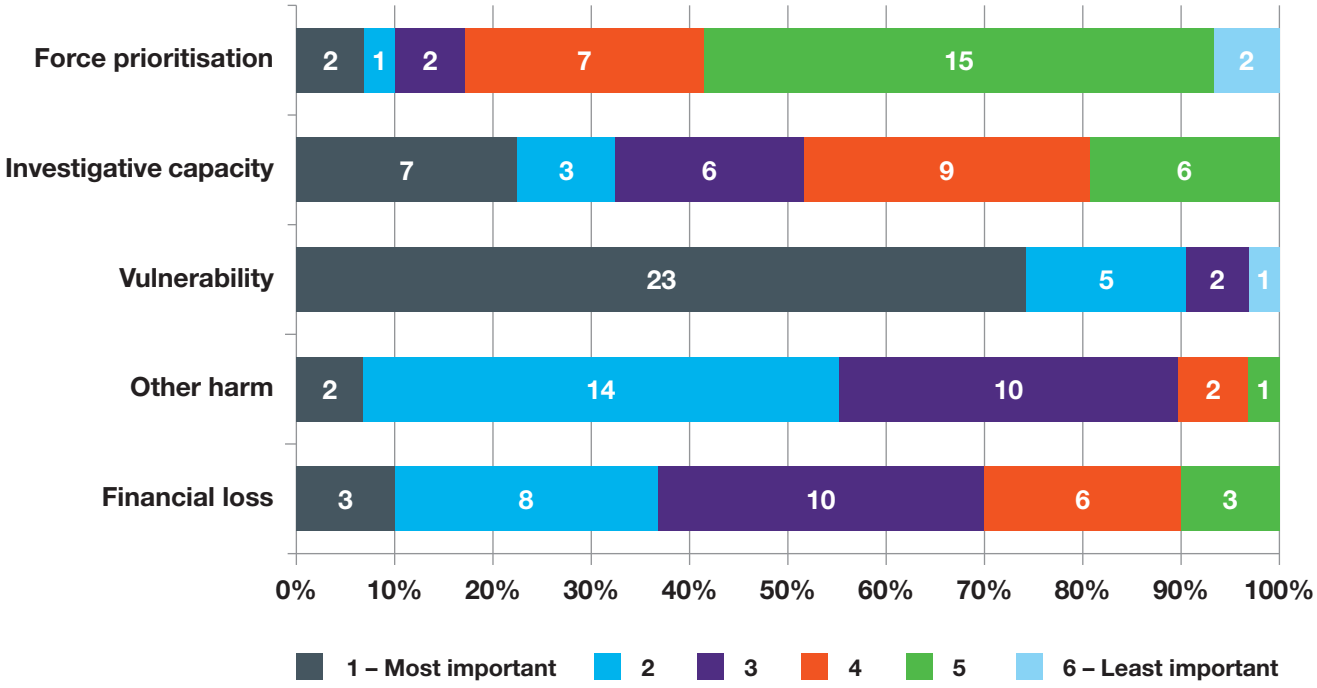
FIGURE 15: Police workforce attitudes on whether fraud should be a priority in their police force.



[50] There were some categories of fraud submitted for manual review due to the perceived seriousness (for example, the value of loss), though many are subsequently found not to be viable (Scholes, 2018).

[51] This survey includes response from officers and staff in Essex, Kent and Avon and Somerset. See Appendix A for more information on respondents.

FIGURE 16: Ranking of different factors for determining whether to investigate a fraud.



* Respondents could provide the same ranking for more than one category.

Figure 16 above shows that from a survey of strategic leads across police forces, victim vulnerability and harm are central to local decision-making for investigation. However as we shall show below both are variably defined and assessed subjectively by practitioners on the ground.

Delays

In 2016-17 the average number of days between a crime report and allocation for investigation or other response was 54 days [52]. Two thirds (66 per cent) of fraud reports that go on to be allocated for any response are done so 60 days or less from the time the crime is reported, only a minority (four per cent) are allocated an investigation more than 180 days (or approximately six months) later. That said, from the perspective of the victim and those assigned to respond, this constitutes a considerable lag in response, potentially spanning months. This not only fails to meet the expectations of victims but can also hinder investigation.

As we shall discuss more fully in Chapter 4 there is a link between these delays and the lack of central capacity to process cases. We make a recommendation on this problem later in the report.

The lack of a framework for assessing threat and harm

There is currently no common framework which would allow the police to triage and prioritise fraud cases in a consistent way.

Apportioning harm values to crime is a challenge (for example see Greenfield and Paoli, 2013). The Cambridge Crime Harm Index or the ONS crime severity scores (Office for National Statistics, 2016b) [53] have adopted sentencing policy as a proxy on the basis that it offers a broad reflection of societal values (Sherman, 2013). However, because fraud is understood and prosecuted under a single piece of legislation (ie Fraud Act, 2006) it is not possible to differentiate frauds on the basis of sentencing measures [54].

Below we set out how frauds might be differentiated by threat and harm. Table 8 outlines a range of variables relating to the potential threat from the offender and the impact their offending is having on victims, which could be used to index the threat and harm at the point a crime is allocated for enforcement, but also as a case unfolds during the course of investigation.

[52] Calculated from the total number of crimes allocated for investigation by any agency in 2016-17.

[53] Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeseverityscoreexperimentalstatistics [Accessed 29.09.2018].

[54] One possibility might be to look at historic sentencing measures to help index variants of fraud but considering the low conviction rate, numbers are unlikely to be sufficient.

TABLE 8: Offender and victim factors for assessing threat and harm on a case-by-case basis.

Offender(s) threat	Victim(s) impact

▪ Number of crimes
▪ Offending period
▪ Offending rate (or speed of offending)
▪ Aggregate loss to linked victims
▪ Scale of impact (borders crossed)
▪ Criminal enablers
  o Money laundering (including use of money mules)
  o Professional enablers
  o Cyber-dependent crime
  o Additional offences (for example, threats or violence)
	▪ Average financial loss to victims
	▪ Self-reported impact on the victim
	▪ Self-identified vulnerability indicator:
	  o Risks losing money
	  o Prior victim
	  o Regular target
	▪ Other vulnerability indicator
	  o Previous reported fraud
	  o Disability

FIGURE 17: An illustrative threat and harm assessment.

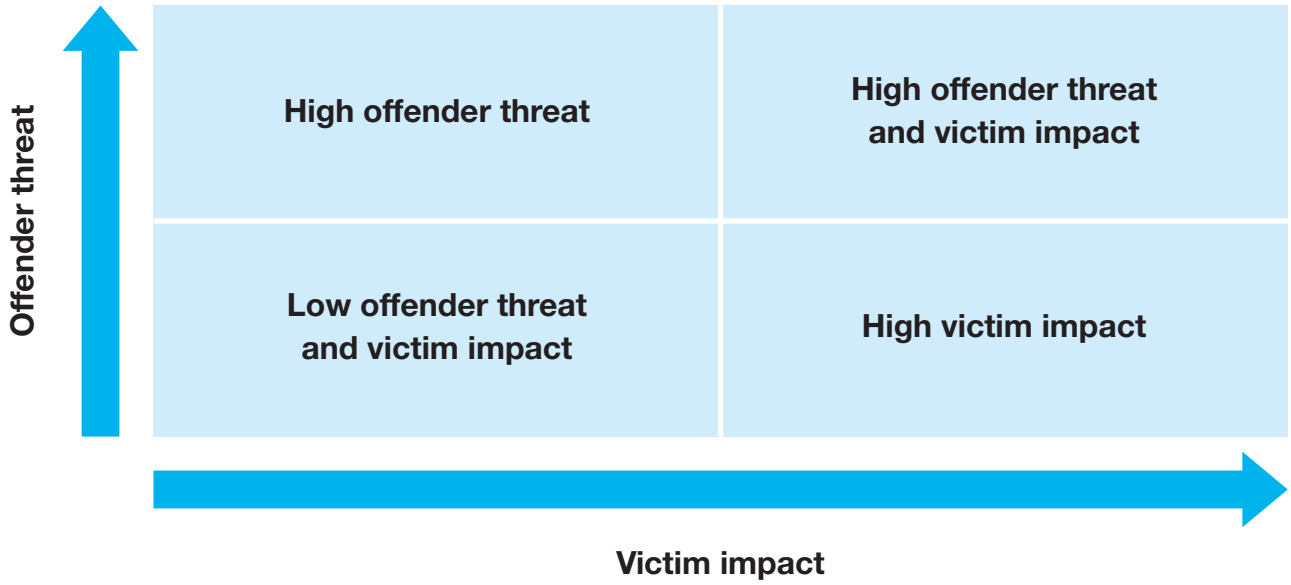


Figure 17 provides an illustration of the way in which these variables, once indexed, could be used to distribute cases on the basis of offender threat and victim impact. Such an index could be used not only to inform prioritisation but also to help guide the nature of the response. To illustrate, cases that fall into the top half of the grid represent complex criminality and are more likely to require specialist investigative resource, whereas those in the bottom right might require more specialist victim support input.

Recommendation 3: The National Fraud Intelligence Bureau should develop a threat and harm index for fraud. This should be used by forces and/or regional units to guide both strategic and tactical decisions.

3.5 LOCAL OPERATING MODELS

There is wide variation in how police forces configure resource which means similar variation in how investigations and enforcement are allocated. Accordingly, police forces adopt different structures for managing local fraud investigations but there is little research evidence as to which approach is most effective. Because of the under-reporting of outcomes in fraud cases it is not possible for us to come to a definitive view on the effectiveness of the different models deployed. However from our surveys and interviews we were able to gain a practitioner perspective of the benefits and challenges of different approaches which we discuss below.

TABLE 9: Police teams closing investigations in Avon and Somerset and Essex in 2015-16 and 2016-17. [55]

Investigation closed by:	Avon and Somerset		Essex	
	Count	%	Count	%
Desktop	518	35%	3	0%
Specialist economic units*	17	1%	42	2%
Local investigation teams	168	11%	260	12%
Local policing teams	238	16%	1645	78%
Other	553	37%	154	7%
Grand Total	**1,494**		**2,104**	

*Specialist teams in Avon and Somerset include the Economic Crime Team and Financial Investigation Unit and in Essex, the Financial Investigation, Money laundering, Retail crime and Commercial Fraud units.

The three police force areas that were a focus for this research (Avon and Somerset, Essex and Kent) each adopted a distinct approach to managing fraud investigations. This is illustrated in Table 9 which shows the distinctions in case allocation between Avon and Somerset and Essex [56].

The models adopted in our three case study forces (including Kent) can be described as ***local generalist***, ***remote generalist*** and ***specialist*** approaches and each is discussed here in turn.

Local generalist model

According to our police force survey, this is a widely adopted model in the police service, with most forces managing fraud enforcement within their 'general' investigative structures and resource. In Essex, for example, all investigations are allocated to a local team (based primarily on where a suspect is thought to be located) which has local discretion for how to respond and prioritise investigations alongside all other investigations.

The benefit of the model is that fraud investigation is spread across all available investigative resource in the force and, on the surface, all fraud investigations are given consideration. However, this model leaves fraud investigation susceptible to a police culture that often fails to prioritise fraud and where many generalist detectives lack the confidence and/or capability to investigate it. Multiple practitioners describe a process whereby fraud investigations can stall due to heavy caseloads and eventually be closed, as described by one local police investigator:

> *'So it all kind of ended up sitting with us and we ended up just having lots of frauds which weren't going anywhere, I think most people in that office would openly admit that they've had frauds sitting in the cupboard not being looked at, gathering dust, for quite a while because they just haven't got time.'*

> *'In general [fraud investigations] are persistently shifted to the bottom of the pile, due to other priorities.'*

This creates widespread inconsistency in decision-making. Once cases have percolated to local teams, they can languish and eventually dissipate, with little strategic consideration of which fraud investigations *should* have been the ones to take forward.

Remote generalist model

This is the model in Avon and Somerset (with a similar approach indicated in a minority of other areas [57]) in which many investigations are initially owned and progressed by a central desktop investigation team tasked to manage fraud alongside other volume crime. The majority of investigators are civilian staff who conduct many of the preliminary enquiries, engaging with external organisations and victims to gather evidence.

[55] This analysis shows only the team which closed a case and does not reflect the priori ownership or involvement of other teams during the course of the investigation.

[56] Kent police force is not included due to data access restrictions.

[57] In our survey of police force strategic leads, three stated all or most fraud investigations involved a desktop investigation team.

Once a case is progressed to the stage where an arrest can be made or evidence seized, ownership is transferred to a local investigator.

This approach shifts the burden of making the preliminary enquiries on to a desktop team with a view to protecting front line resource and freeing them up to deal with other priority areas. However, fraud was treated in the same way as all other volume crimes and staff in the desktop team were given little training or time to investigate. This was described as a challenge for many in the unit who lacked the confidence or capability to investigate fraud and for enquiries which were difficult to turnaround quickly. In addition, once transferred to local investigators, cases faced similar pitfalls as those dealt with by the local generalist model. It also risked a two-tiered approach with the potential for local officers to neglect to investigate referred cases, thereby rendering the prior investigation a wasted effort.

Specialist model

This is the model recently established in Kent police[58] and was also in evidence in some of the larger police forces receiving high volumes of investigations (the Metropolitan and Greater Manchester police). Most police forces have a specialist Economic Crime Team (ECT) dedicated to tackling the most serious and complex fraud cases, however in Kent this constitutes a dedicated hub for dealing with *all* fraud investigations, including 'volume' frauds.

Establishing a dedicated team creates efficiencies by dealing with the problem more at scale. It allows staff to develop skills, experience and the relevant external contacts, which is likely to bring economies in terms of the speed and effectiveness of investigations. This model also means the implementation of more consistent principles by which to assess how and whether to investigate individual cases, thereby introducing greater transparency and accountability within the police force.

However, the sheer volume of fraud cases means there are risks in concentrating investigation resource in one discrete unit, as they may be compelled to adopt 'aggressive screening policies' in order to manage demand. Therefore cases may be closed at an early stage of allocation with little consideration. This was described by one national practitioner:

> *'Having specialists means a much better chance of getting an effective investigation …[there may be] an agreement that it doesn't go down to CID but pretty soon they get saturated … they get saturated very early on.'*

From an effectiveness and efficiency perspective there seems to be some promise in models which pass all fraud investigations through a dedicated hub. We discuss this in greater depth in Chapter Six where we directly address the question of whether local police forces should continue to have primary responsibility for investigating fraud.

3.6 SUMMARY

Judged by conventional criminal justice outcomes the police enforcement response to fraud is poor. Just three per cent of police recorded frauds result in a charge/summons, caution, or community resolution, compared to 13.5 per cent for crime generally. Fraud investigations also take much longer than most other criminal investigations. Low reporting of fraud case outcomes by police forces makes it difficult to come to conclusions about how effectively different forces are handling fraud.

Part of the explanation for these disappointing outcomes lies in the inherent complexity of fraud investigation. Our analysis of fraud case files found a number of challenges encountered in the course of fraud investigations including locating suspects, gathering evidence and engaging victims.

The complex process for allocating cases for investigation presents a further challenge: the quality of information reported by victims through Action Fraud can be poor, inhibiting effective decision-making; there is a lack of clarity around who is responsible for a fraud investigation; the decisions of the National Fraud Intelligence Bureau are detached from the considerations of police practitioners on the ground working to distinct local priorities and pressures; there are major time delays caused in part by a lack of capacity in the system; and the police currently lack an effective framework to differentiate one fraud case from the next. Essentially all this is symptomatic of the gap between those responsible for understanding the problem at the centre and those responsible for delivering the response in local forces.

Police forces use different operating models for managing local fraud investigations. Most forces manage fraud through their general investigative resource, but police officers and staff told us that generalist uniformed officers lack the capacity and the capability to investigate fraud effectively.

[58] Essex police were also planning to adopt a similar model for fraud investigation.

4. THE EXPERIENCE OF FRAUD VICTIMS

Victims who report fraud in England and Wales face a unique reporting landscape and response system. This chapter describes that landscape and assesses the quality of the service provided to victims, looking at victims' expectations of the system, the process of reporting fraud, general services available to all victims and specific support targeted at vulnerable victims. Across this spectrum of response we find that fraud victims experience a service that generally does not meet their reported expectations.

4.1 VICTIMS' EXPECTATIONS OF THE SYSTEM

What do victims of fraud expect from the police and the criminal justice system? Research looking specifically at the expectations of fraud victims has found that victims place a high value on getting their money back and seeing an offender brought to justice (Button et al, 2009b). As we showed in Chapter 3, many victims do not receive a criminal justice outcome. In light of that it is useful to note that victims place high value on the following outcomes as well:

- 91 per cent valued having a single point of contact. 55 per cent rated this of highest importance.
- 91 per cent valued the fraudster being dealt with in another way (rather than a conviction). 71 per cent rated this of highest importance.
- 83 per cent reported that a sympathetic and understanding response was very important.
- 63 per cent highly valued having someone to listen to their experiences.
- 58 per cent reported that help to get over the experience was important.

The most frequently desired type of response was written correspondence and information on progress of the fraud investigation (Button et al, 2009b). Victims' open responses revealed that 21 per cent of victims felt that the most important thing that authorities could have done to help them in their experience of fraud was *'provide updates, preferably regular ones, on the investigation of the fraud, and more detail about how the fraud occurred'* (p.71).

Looking more generally at the needs of victims, Wedlock and Tapley (2016) found, *'...a lack of information can leave victims feeling that their case has been neglected or is not being taken seriously, which in turn can lead to a lack of confidence in the criminal justice system'* (p.13) *'… [what] victims want and require is information to be provided by a consistent, professional source that can provide up-to-date and accurate information relating to the progress of their case'* (p.14).

Though limited, some research has focused on the needs of businesses. The Fraud Advisory Panel (2012) reported that businesses want greater transparency on police decision-making with better advice to guide their decisions on what path to go down (criminal justice or otherwise) to reach a resolution. Federation of Small Businesses (2016) considered the ability of small businesses to cope and recover from the impact of crime and aligned their needs with those of the individual:

> *'Smaller firms should be thought of in the same way as individual consumers across a range public policy issues. This is particularly true with regards to cybercrime...The point is that on a spectrum of characteristics, smaller businesses are closer to individual consumers in many of their behaviours and in terms of degree of market power than businesses that fall into the categories of larger-small, medium-sized and large.'* (p. 24)

As we shall see below these fairly minimal expectations of fraud victims (being kept informed, a sympathetic hearing, a single point of contact and support to get over the experience) are very far from being met in practice.

4.2 REPORTING FRAUD

This section describes the reporting landscape and sets out some of the main weaknesses identified in our research. We look in turn at reporting via Action Fraud, the local police and other public, private and third sector bodies.

Action Fraud

Action Fraud is the central police reporting hub for fraud, launched in 2013 largely in order to achieve improvements in crime reporting and recording, a more coherent intelligence picture and a more rational system

for allocating cases for investigation. Victims can submit fraud reports both through its online reporting system and a call-centre operated during extended business hours.

Action Fraud principally exists to process crime reports but it also provides an initial service to victims who report via the call centre, by assisting them to form a better understanding of what has happened to them, and providing some initial emotional support. Action Fraud is a critical entry point at which needs can be assessed and appropriate referrals made. Call-handlers have an approved list of agencies (for example, bodies to conduct credit checks or regulatory bodies such as the Financial Conduct Authority) to which they can signpost victims to get practical support.

In the course of our research we identified a number of challenges with the way Action Fraud functions as a reporting channel. First, there remains confusion among the public about where to report fraud, despite the existence of a central reporting hub. Research from Citizen's Advice (Couture and Pardoe, 2017) found that awareness of official reporting pathways among those targeted by 'scams' was low, and that 48 per cent of those they surveyed said they would be most likely to report to the police. Less than five per cent named other reporting channels such as Action Fraud, Trading Standards, industry regulators and Citizens Advice. Of those who do not report to Action Fraud, 66 per cent say this is because they have never heard of the organisation (Blakeborough and Correia, 2018).

Second, Action Fraud does not have the capacity to manage the current number of calls it receives. Figures provided by practitioners interviewed in Action Fraud show a snapshot of the level of demand. At the time we received this information there was a 'call-drop rate' of around 30 per cent, a 10 to15 per cent repeat call rate, which was used as a proxy for people who did not get through the first time, and figures showed that in one month only around 28,000 out of 42,000 calls were handled. As one senior practitioner in the Action Fraud contact centre told us:

> *'The demand is breathtaking, if we had double the lines there would be double the calls'*

The call centre retains a public-service focus, prioritising the needs of callers over the time agents spend on calls. However due to overwhelming demand, this results in a tension between managing the number of calls and maintaining the level of victim care.

Third, there are weaknesses in how the system identifies risk and vulnerability among victims. Action Fraud is on the frontline for the identification of vulnerable fraud victims who contact them and can where, appropriate, attempt to refer vulnerable victims to the local police. In practice, the process of identifying vulnerability in callers was unclear, and vulnerability was operationalised as the identification of people with immediate support needs in acute situations or as a consequence of a victim fitting into broad categorisations such as being under 18 years old.

> *'When they say 'I can't handle this anymore', that's a trigger phrase for us'.*

> *'It's such a subjective human thing, some of it is clear elements, for example someone might harm themselves … these* [more obvious cases] *are probably the bulk of what we capture.'*

The process was subjective and dependent on an agent's understanding of the situation. One agent reported, *'there are some that are obvious and others that are a preference'*. At the time of this study, a framework was in development to standardise the operational definition of vulnerability, although this was not available for review.

Fourth, the process for sign-posting victims for further advice, resolution or support can be confusing for victims. There exists what has been described as a support service 'merry-go-round', whereby victims are sent in circles to a multitude of services to get the resolution they need (Button et al, 2009a). Practitioners in the contact centre described frustration from victims when they fail to deliver what they had been led to expect; in some cases due to a lack of understanding from local police practitioners referring the victims. Equally, victims could become frustrated or confused by the array of additional contacts recommended by call-handlers in Action Fraud. One victim support worker described the following:

> 'The victim] *tended to be going around and around in a big circle and not going anywhere.'*

Fifth, once a report is submitted to Action Fraud either online or on the phone, the information victims receive thereafter is subject to considerable delays and is normally minimal. Having reported to Action Fraud victims will receive an automatically generated letter containing their crime reference number and an explanation of the National Fraud Intelligence Bureau process. For many victims calling Action Fraud, the likelihood is that the conversation they have with the agent will be the only time they have verbal contact from any agency regarding the crime. For victims who use the online reporting tool, the likelihood is that the only contact they will receive will be via letter or email.

Currently, the information that people receive regarding their case is limited. Action Fraud aims clarify what victims can expect after reporting:

> *'The NFIB aims to send you an update in writing when your report has been assessed. Updates will only be given three months after your initial report. This is due to the high volume of reports we are currently receiving. Please note that updates cannot be provided by telephone'.* [59]

However, future developments in the proposed Action Fraud reporting tool will provide an enhanced user-friendly 'front-end' system which will allow victims to be able to track their crimes as they progress through the system. Additionally this tool will offer targeted advice relating to the crime.

Action Fraud was originally set up with the purpose of more consistently recording fraud offences, rather than providing a better service to victims. However, given that for many victims it is the only contact they will have with the criminal justice system, it is currently unable to meet the reported minimum expectations of victims.

Recommendation 4: The City of London Police should be given more resources so that it can handle more calls and provide an improved service to victims.

Recommendation 5: The Action Fraud website should provide more authoritative advice and information to guide victims through the services available. It should make online interaction easier, including providing remote advisors who can assess and refer victims where appropriate. It should provide a way for victims to track their case through the system and remain informed about its progress.

Recommendation 6: All bodies collecting fraud reports (Action Fraud, the local police, third and private sector bodies) should work to minimum service standards that cover victims' basic expectations. These standards should be clearly communicated to victims. Given the scale of under reporting these communications should also make clear the value of victims submitting a crime report.

Local police forces

Many people continue to report fraud directly to local police forces, although there is no consistent data on how many do this. 59 per cent of police forces who responded to our survey reported that they did not monitor how many fraud victims contact them directly and two (six per cent) reported that they did not know if this was something they monitored. One local strategic lead said:

> *'This information can be recorded in many different forms. Call takers are confused by Action Fraud processes. All of this results in difficulties in performance monitoring like other crime types.'*

The indication is that a high number of fraud victims contact the police first. For example, while some police forces simply ask callers to call Action Fraud themselves, in Avon and Somerset callers were transferred directly, and they were transferring on average 436 calls each month. The experiences of victims who report to their local police vary depending on the policies and systems in place in each police force and the degree to which an individual call-taker understands the decision-making framework. In some cases contacting the police will make very little difference to the service victims receive, in others it may result in a more traditional enforcement, support and reassurance service. This adds to the confusion for victims about knowing who to contact in what circumstance.

While the local police are not responsible for recording fraud, they have a responsibility to act when there is an opportunity for enforcement or a victim is in need of protection (Association of Chief Police Officers, 2005; Home Office, 2018a). Described as a 'call for service' this is mostly in the event that an offender is still or has recently been physically present or located in the same area as the victim, though there is force discretion and therefore variation in what forces identify and accept as meeting this criterion.

Call handlers responsible for identifying cases which constituted a call for service described the confusing and subjective nature of the decision making process. Standardised assessments were applied (for example, THRIVE [60]) and the victim assessed for a response, but these approaches failed to prioritise fraud. One local call handler described the following:

> *'With burglary we know what the whole process is, in regards to fraud, there is no set process that call-handlers should follow... based on individual feeling and what feeling the person on the phone gets.'*

This is significant because once a case is referred to Action Fraud it can take over a month for it to progress

[59] https://www.actionfraud.police.uk/FAQ.

[60] Threat, Harm, Risk, Investigation, Vulnerability and Engagement is a standardised system for determining the urgency and type of response to callers.

through the Action Fraud system before coming back to the local force (and many will not be followed up by local police). While Action Fraud, notionally, can refer cases to local police forces, they reported some challenges in getting them to take responsibility due to differing priorities and definitions. The opportunities to intervene may have been at the point of initial contact and these may well have been lost.

Call-handlers in one police force reported that any fraud victim who had not suffered a financial loss was referred directly to Action Fraud. However, the degree to which this reflected policy or simply their understanding of the process was unclear, and the decisions they made were free from scrutiny because no auditable record was kept of callers or incidents [61].

Recommendation 7: There should be clear national guidance on what police forces should do when they are initially contacted by a victim of fraud. This should ensure that victims are assessed to determine whether or not their report should be treated as a local call for service, for example, if the victim is vulnerable or if a local offender is suspected.

Other reporting mechanisms

In addition to Action Fraud and the police there are several statutory, charitable and private bodies that either receive reports of fraud, provide some form of victim service themselves or direct the victim towards Action Fraud.

In partnership with Trading Standards, the Citizen's Advice consumer service provides advice for consumers, including those who have been defrauded and can be contacted via a telephone service or a web form. The information provided by consumers contacting the telephone service is assessed by call handlers who determine whether to pass it to Trading Standards. Trading Standards then decide what action, if any, to take depending on local priorities and resources, and may contact the consumer directly or refer and work with police depending on local partnerships and relationships. The consumer service call handlers may also signpost victims to other services such as Action Fraud or Age UK.

Customers who are defrauded and have contact with their bank or other financial service provider can still report to Action Fraud, whether their bank resolved their issue or not. The processes in the private sector for assessing victim support needs are mixed or absent and it is not known how many victims go on to receive support from the police or other services. Banks and other financial services share crime information with the National Fraud Intelligence Bureau, or pass data to Finance UK or Cifas as part of an industry arrangement.

Cifas is a not-for-profit fraud prevention membership organisation with over 450 members from private (such as financial and telecoms businesses), public and the charities sectors. It has its own system for categorising fraud reports in a database of high risk fraud cases with details shared across its membership bodies for the purposes of preventing further fraud. This information is shared with the National Fraud Intelligence Bureau to help build a more comprehensive national picture of fraud offending and augment the intelligence, as well as share the details of victims recorded on the system by member organisations. However these reporting parties are not treated as crime victims and are not assessed or disseminated to local police forces. For those compensated, victim status is transferred from the individual to the business and it is unclear what if any assessment of support needs is completed by the service provider.

The fragmented nature of this landscape poses its own challenge for encouraging fraud reporting and properly responding to it. The many organisations who receive reports operate largely in isolation from one another and create a complex landscape of services that victims may need to engage with in order to get their needs addressed. This multiplicity of bodies presents a challenge for many victims (or even professionals) when they are deciding who to contact. In the case of fraud, the service the victim engages with will ultimately determine the support they will receive.

Recommendation 8: The public should be made aware of the different reporting channels, and in what circumstances they should be accessed, so that they can access the service most appropriate to their needs.

4.3 VICTIMS' SERVICES

This section describes and appraises the range of services fraud victims may receive after reporting their crime. We discuss the support provided to those identified as vulnerable in the next section.

Victim services from the police

The police (locally or within Action Fraud) are responsible for providing a basic service to victims of crime. Where this is provided for fraud victims this commonly involves

[61] Audio records could be checked on a case by case basis by supervisors but this could not be done specifically for fraud calls.

giving advice and signposting to organisations or websites that may be able to address their needs or provide prevention advice. Most of the services and support available is broad and generic. Victims are referred to Victim Support, Citizens Advice, Social Services, Trading Standards, Cifas, and in some police forces, internally to local PCSOs who carry out a visit and conduct vulnerability assessments. Referral organisations largely work in isolation from the police and have their own criteria for acceptance.

Some police practitioners emphasised that a successful outcome should be defined as providing a good service to the victim rather than achieving a successful investigation. This acknowledges the diversity of victim needs and the value the police can bring in delivering advice and making clear the decision-making in relation to investigation.

Police practitioners who we interviewed or who responded to our surveys described the following forms of good practice:

- Keeping victims in the loop during what can be long drawn out investigations, *'The uncertainty of what's going on can be upsetting… I try and tell them, 'I've sent this off to the bank, I'm waiting for the bank, it'll probably take eight weeks so don't worry if you don't hear from me in those eight weeks'*.
- Open and honest communication.
- The benefit for some victims of being able to have a conversation with a uniformed officer.
- Timely and appropriate engagement – *'what they want is quick-time engagement over the phone'*.
- Providing opportunities for the victim to be heard, *'...of the fraud victims I've dealt with, I've felt they've gotten closure when they've given a Victim Impact Statement… they get to have a voice, for some it's had a drastic effect'*.

The service the victim receives from the police will differ according to whether they have reported the fraud directly to the police in the first place and whether or not their case is allocated for investigation.

Call for service

In our national survey, police forces were asked about provision for victims who contacted the police directly. 47 per cent reported that all or most fraud victims who contact them will be referred to Action Fraud, however, one in five police forces visit all or most fraud victims who make direct contact with them (see Figure 18). Feasibility for doing this is likely to vary depending on the size of the police force and number of victim referrals received each month, as indicated by one strategic lead in a police force receiving high volumes of reported fraud:

> *'How big does our victim support team need to be? … where do I find the cops to do those visits?'*

Victims without an investigation

The names of most local victims are presented to their police force via a list issued by National Fraud Intelligence Bureau (NFIB) on a monthly basis [62]. The majority of the victims on this list will not receive a police investigation. Our research identified police forces who make little or no use of the NFIB victim data and thereby fail to acknowledge local victims that, from a procedural perspective, are linked to crimes that are 'owned' by the City of London Police.

Because of this, a significant number of fraud victims receive no follow-up or offer of support, including vulnerable victims. Evidence suggests that some police forces do not even access or record the information on fraud victims provided by these lists onto their systems.

> *'If there is a victim in* [force area] *but there is no local suspect, we'll never hear about it … we can access it* [the information]*, but we don't.'*

Figure 19 shows the results of the survey of forces which indicated that a significant proportion were not offering any service to these victims.

Victims linked to a police investigation

Due to the digital or otherwise remote nature of fraud offending, the police force allocated an investigation by the NFIB is generally not where the victim is located, but where the suspect is located. Victims commonly reside outside of the jurisdiction of the investigating police force and this introduces distance between an investigating officer and victim. Some practitioners expressed concern that although the investigating force was responsible for offering the victim a service it does not always occur. The victim is entirely reliant on the approach and processes of a police force in other areas of the country.

The remoteness and high volume of victims that can be linked to an investigation can be challenging for a practitioner to manage. To illustrate, one victim support officer given responsibility for supporting victims through a trial described the following:

[62] New IT systems under development will mean these will be delivered in real-time to police forces.

FIGURE 18: The response to victims contacting police forces directly.

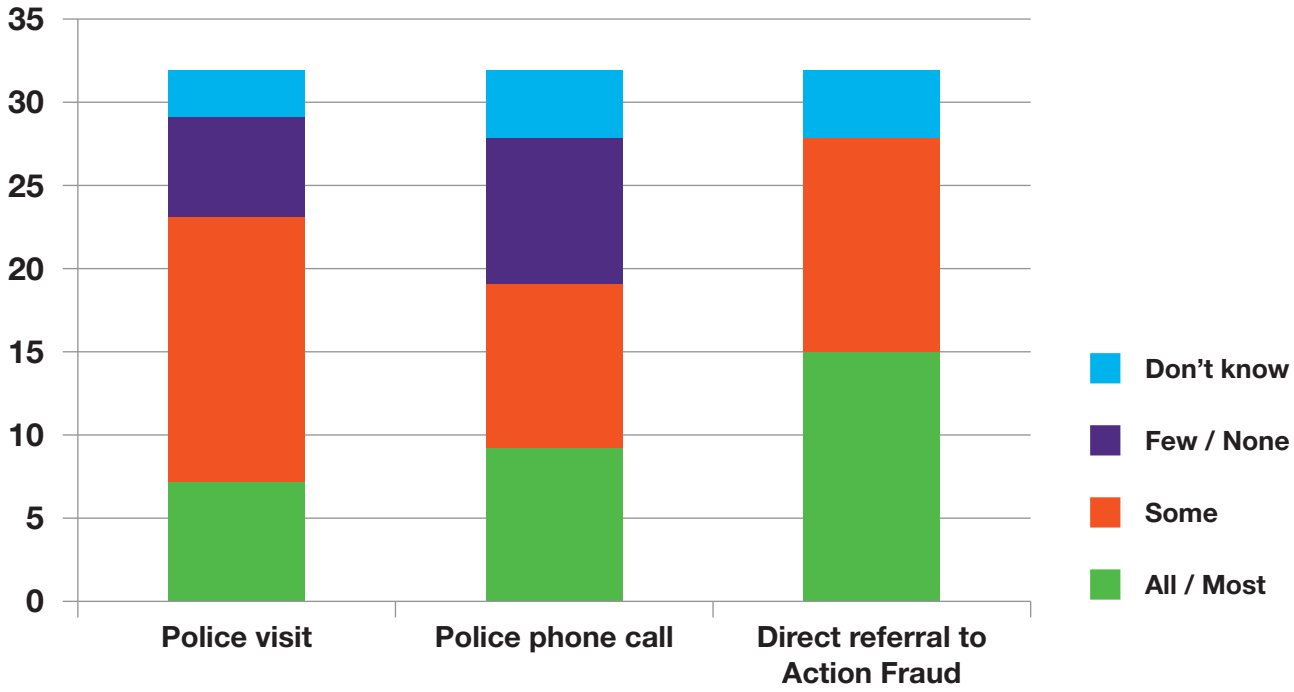
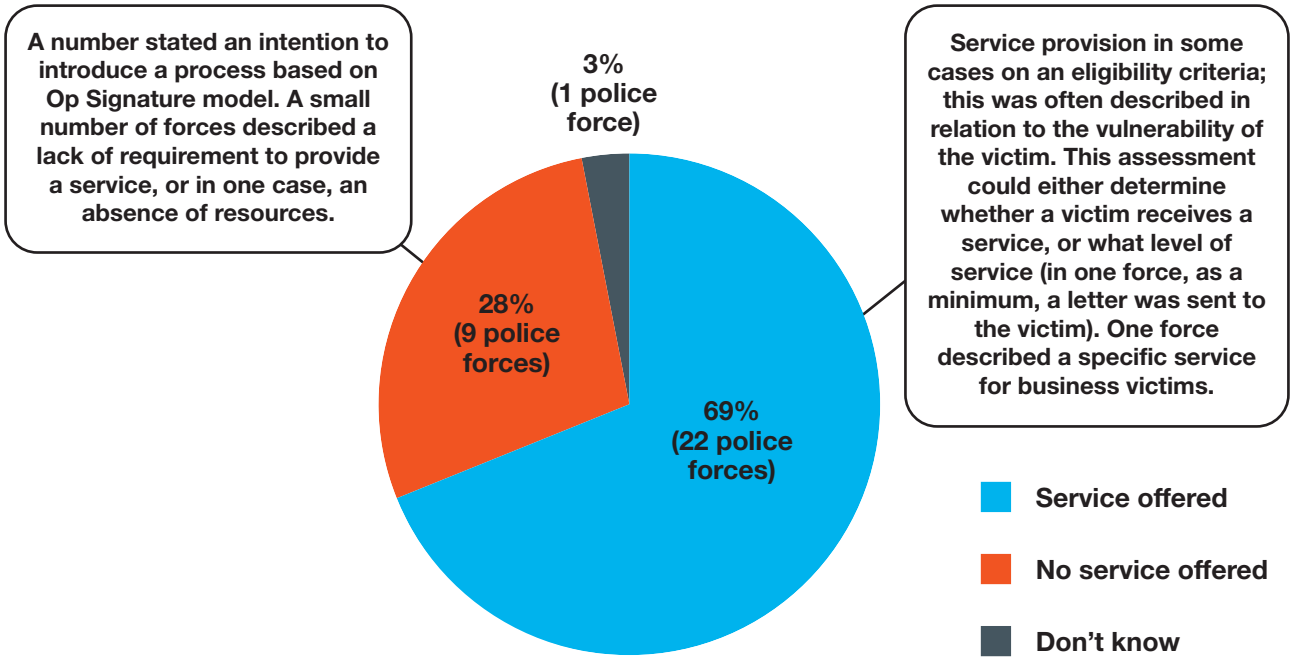


FIGURE 19: The service offered by police to local victims not allocated an investigation.



'I've had a case where there's 50 victims… we even had one in Spain, Northern Ireland, literally they were everywhere.'…'you don't build as much of a rapport as you do with victims of smaller cases, which means it's then harder to find out what the victim needs.'

Some practitioners highlighted the importance of providing a service to non-reporting victims:

'We should be proactive with regards victims who we identify haven't reported – they are more likely to be targeted again than anyone else; we should not carry on just fire-brigade policing, tending to the person who complains the most.'

The need to manage the demands of engaging with victims uncovered as part of an investigation had resulted in a variety of responses from forces, including in some cases a 'pro forma' response where victims are sent a letter and asked to respond, or even a dip-sampling strategy, where contact will be made with only a proportion of victims. These limited attempts to engage or acknowledge people who are potentially

victims and at risk, is a result of a need to make a pragmatic decision in the face of limited capacity:

> *'If you* [the victim] *choose not to respond, I'm going to decide as the SIO that you're not worried enough to count as a victim yourself.' '"We think you've been a victim, we've arrested some people", I would expect that person to come forward … but I've got to sit there and think if it's really worth the time chasing them up.'*

There were examples of work to address these demands, mostly arising from within specialist teams who had made bids for dedicated victim support resource, but this practice was not mainstream. One investigation by the Regional Organised Crime Unit, where 4,000 potential victims were identified, highlights the scale of some offending and the resources needed to identify and provide appropriate care.

In this case the team managed to procure a victim care officer from a local force who followed up with victims who had responded to letters, and which included a questionnaire which assessed their potential vulnerability.

Recommendation 9: There should be a national minimum standard of service available to all fraud victims whose cases are being investigated.

Victim support services

All victims of crime have a right to access victim support services to help them recover from the effects of a crime (Ministry of Justice, 2015). Action Fraud is responsible for providing this service when victims report a fraud, which is subsequently delivered by a local service. In 2016-2017 statistics from one of the largest local victim service providers [63] (Victim Support) show 35,220 victims engaged with the service. However, 89 per cent of victims subsequently chose not to engage when contacted by the local support provider.

We have found that there is considerable variation in the proportion of victims engaging in different geographical areas, for example, although Sussex and Essex receive a similar number of referrals (n=1,139 and 948 respectively) the level of victim engagement in Sussex is one in five (n=194, 20 per cent) while in Essex it is just one in twenty (four percent n=51).

It is notable that in areas where police forces have placed considerable strategic priority on supporting and protecting elderly victims of fraud, higher proportions of victims were engaged, for example, in Wiltshire and Sussex. This shows that while the receipt of support is premised on victim choice, provision is strongly influenced by the priority or investment in delivering this support locally.

Figure 20 shows the number of referrals for support in the 43 police force areas, and the percentage of victims in the area who subsequently engaged with Victim Support.

Figure 21 provides a breakdown of the type of support offered to fraud victims by Victim Support in 2016-17.

We identified concerns from police and support service practitioners that generic victim services are failing to deliver an effective service to victims of fraud:

- Some local practitioners told us there should be improved processes for assessing the needs of victims at the point of reporting so that this support is directed at *'the right person who wants a service'*. Victims at this early stage are generally focused on eliciting a police response, getting their money back or other practical intervention and receive an offer of a victim's service they do not fully understand. As Figure 21 opposite shows, most victims services focused on providing emotional support, which for many is not what they are looking for. One local support worker felt Action Fraud *'were not explaining the service properly …* [a need to explain] *it's emotional support'*;
- There are delays in access, often of over a month, between the time a victim accepts the support and is subsequently offered it.
- Victim support services are focused on all crime victims. The support is generic and unlikely to focus specifically on vulnerability, addressing complex needs or the risks of repeat victimisation. Specific training for providers is limited and there are few systems to identify and address the needs of fraud victims who will require more intensive support.

The indication is that a service restricted to providing generic victim support is poorly equipped to meet the needs of fraud victims.

Recommendation 10: Action Fraud should make clear to victims what they can expect from when they are referred to a local victims support service.

[63] The commissioned service provider can vary by police force therefore these statistics are not representative of all 43 police forces.

FIGURE 20: A comparison of the number of fraud victims who opted to receive support (2016-2017) and the proportion who subsequently engaged with Victim Support, by police force area. [64]

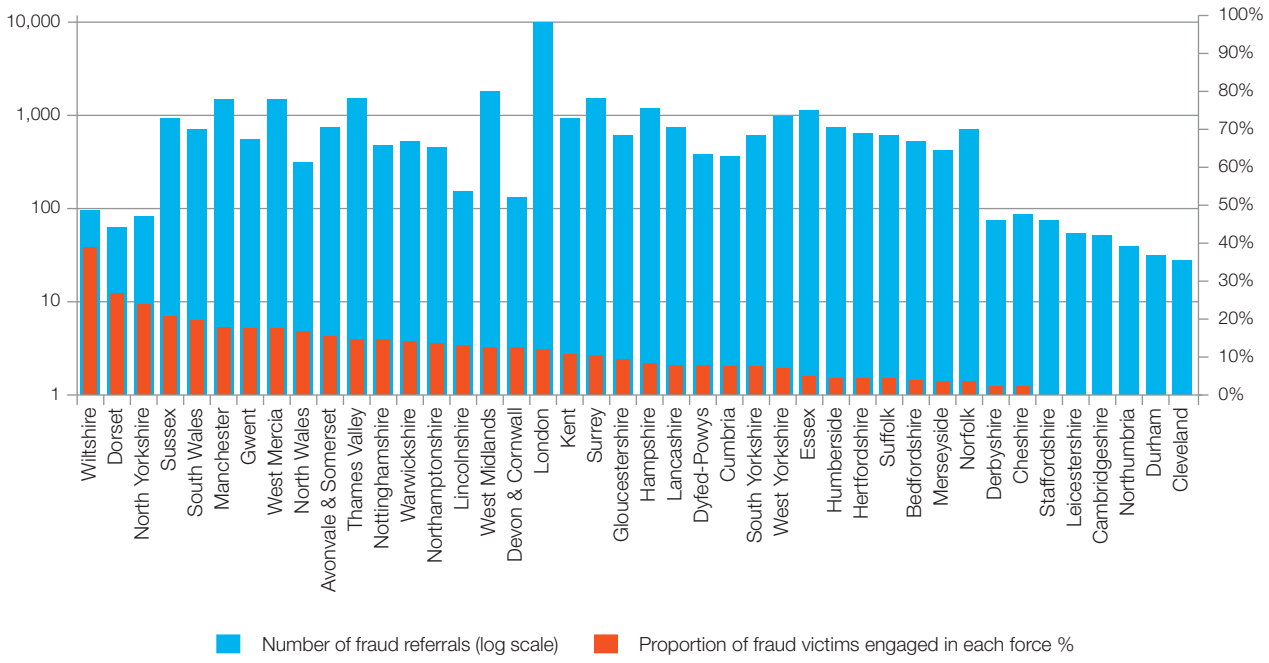
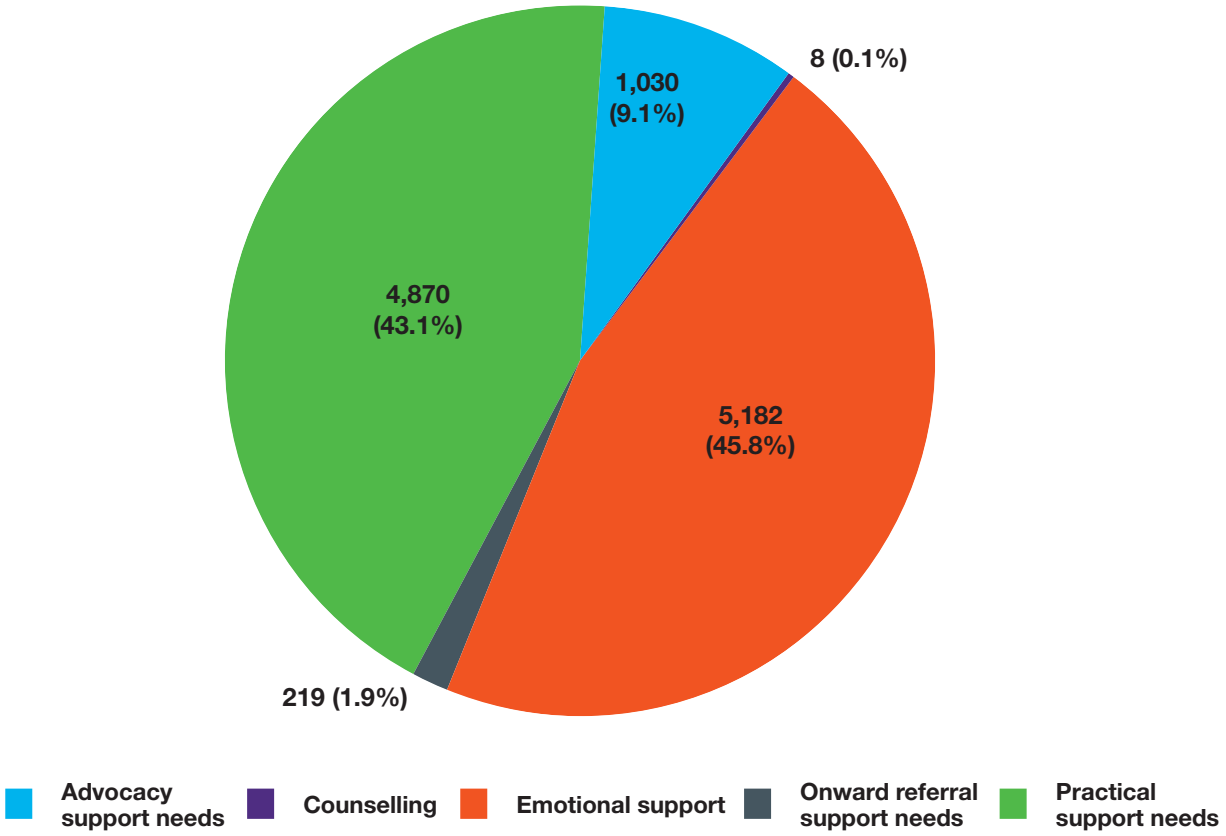


FIGURE 21: The types of support offered to fraud victims by Victim Support in 2016-17.



[64] Since devolution of control to Police and Crime Commissioners a number of police forces have elected to provide all or some of their victim services in-house, which explains why Victim Support received no referrals in a small number of police force areas.

4.4 SUPPORT FOR VULNERABLE VICTIMS

There is now an increasing recognition of the needs of vulnerable people in relation to fraud. Analysis of police and crime plans (2016-17) found references to tackling vulnerability in all 43 police forces and in 17 (40 per cent) there was explicit reference to vulnerable victims of fraud. The identification and prioritisation of vulnerability as part of the police response to fraud is still in its infancy, but in some police forces this vacuum in service provision is beginning to be filled, particularly for victims whose cases were not allocated an investigation.

Our national survey of police leads for fraud, showed the characteristics and experience of the victim to be the most important factors for determining the provision of victim services. Table 10 below shows how a number of factors that overlap with vulnerability are taken into consideration by forces, including victim characteristics and likelihood of repeat victimisation; nearly all described these as either very or somewhat important (97 and 100 per cent respectively). Fewer perceived the specific characteristics of the offence as being of similar importance.

Some police forces are now introducing systems for identifying vulnerable victims and providing them with a dedicated service. Before going on to describe these services we first look at how the police go about assessing harm and vulnerability in relation to fraud and set out how this could be improved.

Understanding vulnerability in relation to fraud

Previous research has taken a macro-perspective of the likelihood of people falling victim to fraud based on certain attitudes and behaviours (Home Office, 2016; National Fraud Authority, 2011). However, empirical research on fraud victims and understanding who might be considered *vulnerable* has thus far been lacking – who they are, their risk profile and their needs. An inability to pinpoint how vulnerability is manifested in fraud victims creates a barrier to effectively steering resource towards need.

Definitions of vulnerability, and corresponding practices, vary across police forces and the wider fraud response system which creates a lack of parity and leaves some victims with unmet need. A prominent definition for determining service provision is the eligibility criteria in the Victims Code of Practice which singles out victims on the basis of the severity of the crime experienced, whether the victim is 'persistently' targeted, is under 18 or has a mental or physical impairment (Ministry of Justice, 2015). Importantly, these indicators seldom apply to the fraud victim group and in recognition of this some police forces are developing bespoke frameworks for identifying fraud victims who are 'vulnerable'.

The reporting process has depersonalised local police forces' contact with victims; the majority of victims are presented to them in the form of data in spreadsheets (shared by City of London Police) rather than in person. The process of identifying vulnerability is therefore reliant on data analytics, an approach known to have limitations compared to more personalised assessments (Innes and Innes, 2013). The likelihood that someone is assessed as vulnerable through these processes is contingent on a number of factors that pertain more to systems and protocols, than to the status of the victim themselves:

- **Where the fraud was reported**: there is variation in the priorities, tools and definitions across local police forces, Action Fraud and other organisations (eg Trading Standards). There is increasing emphasis on online reporting, especially via Action

TABLE 10: Factors for determining the provision of victim services in a police force

	Very important	Somewhat important	Not very important	Not at all important
Characteristics of victim	25 (78%)	6 (19%)	0	1 (3%)
Harm to victims	22 (69%)	10 (31%)	0	0
Likelihood of repeat victimisation	24 (75%)	8 (25%)	0	0
Type of fraud reported	5 (16%)	16 (50%)	11 (34%)	0
Specific characteristics of modus operandi	6 (19%)	15 (47%)	9 (28%)	2 (6%)
Other assessed vulnerabilities	9 (69%)	2 (15%)	0	0

TABLE 11: Categories of vulnerability described by practitioners.

Personal Factors	**Knowledge** – Individuals entering into situations or transactions where their limited experience and knowledge can be exploited. Most frequently, this related to online activities, for example banking or dating, that they were more used to negotiating offline (and where they might be better able to judge the risks). These individuals were not alert to fraud indicators and were also more likely to engage in risky behaviour, for example responding to pop-up adverts for investment advice. **Trust** – A lack of familiarity with current custom and convention results in situations where people are more inclined to trust people behaving fraudulently. This was often perceived as a generational issue, where older members of the population were more likely to view sales contact by telephone or on the doorstep as acceptable, or, contact by phone from a person purporting to be a police officer to be legitimate.
Situational Factors	**Social isolation** – Social isolation was perceived as a key factor in both a person's susceptibility and resilience to victimisation. Social isolation was most frequently described in relation to elderly people living alone. People's desire to reduce their isolation was perceived to increase their vulnerability to fraud victimisation, by increasing the likelihood that they would respond to messages or engage with fraudsters. Another key aspect of social isolation was the way in which it exposed people's vulnerability; social support has a protective factor in minimising risk attributable to a person's vulnerability. For example, a fraud victim who was maintaining a successful career working full-time in IT succumbed to doorstep fraudsters only once his parents had died, leaving him to live alone and manage the household. The desire to maintain a rewarding relationship may prolong and increase a victim's exposure to fraud; *'his primary concern was not losing the scammer's friendship...'*. **Community** – The physical or digital communities within which an individual lives may increase their susceptibility to fraud victimisation. For example, practitioners observed that fraudsters targeted areas where there were high concentrations of residents with perceived vulnerability, eg. park homes, where elderly people are more likely to live, and university students living in halls of residence. **Financial status** – For example, victims who release their pensions early may be targeted by investment fraudsters. The resilience of the individual is also affected by a person's ability to absorb or restore the amounts lost (a challenge for elderly victims who no longer work). Individuals with low incomes can also be targeted and relatively small losses can be harmful for example, students who are facing increasing financial pressures and so can be susceptible to recruitment scams, or those facing financial pressure falling victim to loan-lender fraud.
Incidental Factors	**Inability to access support** – People targeted by fraud frequently experience shame and embarrassment.A theme of self-blame was apparent in the accounts of people providing support to victims of fraud. This was in part because people's *'behaviour is linked to the crime itself'*. This is compounded by attitudes towards fraud victims, *'Some people know they're going into a dodgy deal but they go ahead anyway'*. This restricts the victim's ability to seek out support, and this was particularly true for some older victims who felt a pressure to show that they were capable of independence; *'they don't want family to know and think that they can't cope'*. **Previous victimisation** – People who have been previously victimised are more vulnerable to fraud victimisation. This may be because fraudsters have their details which may be shared with other fraudsters (*'it's like a grapevine'*) or the victim is motivated to get their money back and responds to fraudsters offering to recoup their losses. **Grooming** – People who have been groomed by fraudsters, can be particularly vulnerable to re-victimisation because of their desire to maintain what they perceive is a legitimate business or personal relationship. This can prevent them from realising they are a victim and consequently limit access to support and advice.

Fraud, which precludes real-time assessment and is dependent on the victim providing relevant information.

- **The information recorded**: The quality of information is dependent on call-handlers' understanding or online self-reporting. Subsequent identification of vulnerability is contingent on accurate categorisation and inclusion of relevant contextual detail to assist follow-up analysis of the data. Action Fraud was observed during fieldwork to construe vulnerability primarily in terms of immediate risk of physical harm (eg suicide)[65], which did not correspond with the vulnerability criteria deployed in some police forces.
- **Victim care protocol**: many frauds are not investigated and the decision to undertake assessments of victims in these cases is dependent on the divergent policies and protocols in each police force. Each police force prioritises fraud differently and is adopting discrete processes for identifying it. Consequently, a victim identified as vulnerable in one location may not be identified in another. Our survey indicates at least nine forces make no attempt to identify the vulnerability or need of local victims not assigned an investigation.
- **Practitioner understanding**: there was a widespread lack of clarity among for practitioners in the police, and partner agencies, about how to identify vulnerability in the context of fraud.

Table 11 sets out a range of factors identified by practitioners as contributing to the vulnerability of fraud victims they had worked with. This list of categories is unlikely to be exhaustive as it reflects the subjective experience and perceptions of practitioners in enforcement and victim services.

A number of the factors in Table 11 were evident in existing police models identifying vulnerability but in some cases identification was done by proxy, for instance viewing anyone over a certain age as vulnerable. However, as the victimisation data in Chapter 2 demonstrates, while elderly people may be more vulnerable to certain types of fraud this is not true across the fraud spectrum. A charity representative commented, *'lots of old people can be affected* [by fraud]*, but not all old people are vulnerable'*, as it is dependent on a range of contextual factors such as those outlined above.

Limitations in the data and the blind-spots that are created by an over-reliance on generic vulnerability frameworks (eg the Victims Code of practice) remain a challenge when understanding vulnerability in relation to fraud.

Recommendation 11: There should be a national framework for identifying, assessing and prioritising fraud related vulnerability. All police forces, regional units and Action Fraud should use the same criteria.

Services provided by the police and partners to vulnerable victims

Two models of police practice have emerged in regard to identifying and supporting vulnerable victims of fraud, a local model and a more centralised model. While there are challenges in conducting robust victim assessments they represent positive steps towards addressing a significant gap in service, especially for fraud victims not allocated an investigation. In particular, the Economic Crime Victim Care Unit demonstrates how a personalised victim-focused response can be delivered remotely by a hub of specialists, and the model is generating interest from forces.

Op Signature

Originating in Sussex, Op Signature is recognised as best practice by HMICFRS for working with vulnerable victims of fraud. It focuses on the identifying and supporting vulnerable members of the community, with the aim of protecting them from future harm. It is a packaged policing response provided to vulnerable fraud victims who call the police, are referred by Action Fraud, identified in police and partner intelligence or who are non-reporting victims who first responders on the ground may come into contact with. Op Signature has engaged a wide range of local partners including Trading Standards, adult social services and third sector support organisations. In practice the focus has remained largely on elderly members of the community and vulnerable victims who are identified in the data on the basis of being over a certain age[66].

The model has been adopted in various guises across the country to address a lack of service for local victims (and in particular as a method for identifying victims' vulnerability and need from data provided by National Fraud Intelligence Bureau) – although some practitioners expressed doubt over whether the same model can

[65] At the time of our visit, it was indicated that a more comprehensive framework for steering questions on vulnerability was being developed.

[66] Victims who have reported a crime are screened on the basis of being aged 70 or older.

feasibly be adapted for use in forces with high volumes of fraud and different victim profiles.

National Economic Crime Victim Care Unit

This victims unit operates remotely to support vulnerable victims in three urban police force areas (the Met, West Midlands and Greater Manchester Police), the Economic Crime Victim Care Unit (ECVCU) has a similar function to Op Signature through centralised systems and contact. The ECVCU assesses victim data collected by Action Fraud on victims in three police force areas, to identify potential vulnerability and passes these cases to advocates in the team who make phone contact with victims.

It adopts similar principles to Op Signature, by identifying from high volumes of victim data who is most likely have the greatest level of risk or need, using at the time, slightly less structured assessments of the information provided by National Fraud Intelligence Bureau. On contacting victims, advocates use a standardised tool to identify riskand vulnerability in victims and assess their needs. The service is bespoke and provides victims with tailored advice and guidance; it looks at how to address issues causing vulnerability and how the victim might be supported. *'They build up trust, some of them haven't told anyone, they haven't even told their children'*.

Victims are given a phone number for their advocate, and can access the service, *'as long as they need'* it, in practice contact can be maintained for up to two to three months, but the majority of victims do not require this level of service. Victims can also phone back at a later date should they be concerned about potential fraudulent activity. The nature of a dedicated team allows for the development of expertise regarding the needs of fraud victims and centralised knowledge of locally available support. The unit demonstrates how a personalised victim service can be delivered within a centralised model.

Both these models represent progress in recognising harm and vulnerability among fraud victims. Op Signature is constrained to operating from within forces, which have scarce resources for tackling fraud. The ECVCU offers a dedicated service delivered remotely, and in principle, by establishing links in the local area, draws on local services when necessary to support or protect a victim. Both are focused on a small number of victims assumed to have the most acute level of need.

In addition to the police, there is a range of statutory and third sector services operating to different remits, protocols and thresholds in supporting individuals at risk from fraud. These are described below.

Adult social services

Adult social services have a remit to protect vulnerable adults from financial abuse. They work to definitions in the Care Act (2014) that can be used to assess for care needs such as a physical or mental impairment. In terms of mental capacity, the vast majority of fraud victims do not meet the criteria for safeguarding as described by a regional Trading Standards scams officer:

> *'You've got to have a significant detriment to have no capacity … the vast majority fall short of the threshold.'*

One practitioner described a tendency for social services to focus on financial abuse in instances where the offender was present rather than when victims were targeted remotely (for example, by post). As with other services, the scale of demand has the potential to outstrip available resource.

Trading Standards

Local Trading Standards offices have carried out innovative work with fraud victims and in some localities have developed good working relationships and sharing agreements with police forces. However, their resources are low, and work is dependent on local priorities and individual interest. Research by the National Audit Office (2016) reports that Trading Standards have nowhere near the resource required to deliver a service to victims who are suspected to be vulnerable.

Third sector support

Other third sector agencies, primarily special interest organisations working on behalf of their target demographic (eg Age UK) and have some potential for provision, though there is a wide variation in their capability to do so. A good example is an Age UK partnership with Economic Crime Victim Care Unit which is running a pilot scheme in a number of London boroughs, providing one-to-one and group awareness raising to encourage reporting and prevent fraud victimisation. Age UK also works with vulnerable people, particularly those responding to scams. The police refer victims over 55 to Age UK, who follow up with the victim. The pilot focuses on victims who are not being allocated an investigation or receiving support. There were initial concerns about the scale of demand, but this has been lower than anticipated, with 200 victims referred over six months in four pilot areas. The pilot offers guidance, practical support eg help with benefits, befriending, and aims to engage people with local services.

Recommendation 12: All fraud victims who are identified as vulnerable should receive at the very least a follow up call from their local police force.

Recommendation 13: The Home Office should fund an expansion of the Economic Crime Victims Care Unit to cover all police forces to provide a baseline of sustainable provision for identifying, assessing and supporting vulnerable victims of fraud. The Unit will make referrals to the local police force for further action where appropriate.

4.5 SUMMARY

Victims of fraud have some fairly basic expectations about what they should receive from a service, even in the event that they will not get their money back or that the offender is not detected. Victims expect to be kept informed, to be listened to, to be offered support where appropriate and to have a single point of contact.

The response system currently falls far short of providing this basic level of service.

While the creation of Action Fraud was essential to form a national repository of crime and intelligence data, by divorcing the response from local services, it left a void in the service for victims who wanted or needed advice, reassurance or support. While functional, it created an impersonal service insensitive to the needs and wants of those victims who required more help or protection.

There is still a fragmented reporting system with varying standards of service that can be confusing for victims. Many victims still report to their local police in the first instance and forces have varying approaches to these cases. In some instances this can mean that signs of vulnerability or opportunities to investigate local frauds are missed.

Fraud victims experience highly inconsistent support from the police once they have reported. Some police forces do not even look at the data they are sent by the National Fraud Intelligence Bureau on their local fraud victims. The service victims who are allocated an investigation receive is patchy and inconsistent, delivered by an investigator often on the other side of the country who might be struggling to keep in contact with large numbers of victims. Victims who opt to be referred to a generic local victim support service often find that this does not meet their needs.

There is no specific framework for assessing vulnerability in relation to fraud and there is no consistent understanding of it by practitioners. Different forces have different policies on whether, if at all, to contact vulnerable fraud victims in their area.

We have made a number of recommendations, all of which aim to provide a consistent set of national standards as to what victims of fraud can expect. National standards are required because of the remote nature of fraud offending which means victims have to navigate agencies and police forces in different parts of the country. The aim should be to provide a single seamless service to victims of fraud with the same basic standards wherever they live.

5. PREVENTING FRAUD

Prevention is better than cure and this is as true for fraud as it is for other types of crime. Given the sheer difficulty of bringing fraudsters to justice very many practitioners told us that most of the emphasis by the police and others ought to be on prevention. In this chapter we appraise what the police and their partners currently do to prevent fraud. We do not cover the whole prevention landscape and focus only on those areas of preventative work in which the police play some part. For this reason we do not examine the whole area of commercial regulation or security standards in industry to 'design out' crime at source. Rather we focus on the work of the police and their partners nationally and locally to prevent fraud, mainly through education and awareness campaigns and targeted work with vulnerable people aimed at changing victim behaviour.

5.1 WHAT IS CRIME PREVENTION AND WHAT ROLE CAN IT PLAY IN TACKLING FRAUD?

The concept of crime prevention

The United Nations defines crime prevention as:

> *strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes. (UNODC 2010: 9)*

Crime prevention is an attempt to reduce and deter crime (Sherman et al, 2002). Other secondary benefits, or 'diffusion' of benefits may also be observed, including a reduction in crime in adjacent locations (Clarke and Weisburd, 1994); a reduction in the fear of crime and better quality of life (Weisburd and Eck, 2004); increased public support for policies (Roberts and Hastings 2012); and reduced costs to society (Farrell et al, 2013; Welsh, 2018).

Support for a focus on fraud prevention was a recurring theme in our research. For example, fraud specialists in the police and the NCA were strongly supportive of shifting emphasis to preventing fraud based on the principle that it is impossible to 'arrest our way out of it'. Some noted:

> *'The City of London Police could have a thousand investigators and it still would not make much of a difference, the answer needs to be prevention.'*

> *'If the measure of performance was the amount of money lost or the human cost, then I wouldn't put a single bit of resource into investigation, it would be prevention … resources would be far better [used] in preventing the fraud in the first place ... but very few [police] forces put anything into prevention and that's got to change.'*

Crime prevention techniques applied to fraud

Much police work on crime prevention in the UK has built on the work of Ronald Clarke who argued that one of the main ways of preventing crime is to reduce the opportunity for it (Clarke, 1995; Clarke, 1997; see for discussion of crime prevention, Bjorgo, 2015; Ekblom, 2011). This framework is based on the premise that offenders are, to a large extent, rational thinkers and will weigh up the risks and rewards before engaging in crime (Cornish and Clarke, 1987, 2002 and 2008; Tilley and Farrell, 2012). So the logic goes, in so doing they will decide not to commit offences if the costs or risks outweigh the rewards.

Over the years the framework has been developed and modified and now consists of 25 techniques which can be applied to different types of crimes. The five main principles of situational crime prevention are:

- *Increasing the effort* required to commit crime by reducing the opportunities for committing crime or making it more difficult to be successful.
- *Increasing the risks* of crime by creating situations that increase the chances of the offender being caught.
- *Reducing the rewards* by decreasing the benefits to offenders.
- *Reducing provocations* by reducing the frustrations and stress that may lead to poor behaviour.
- *Removing excuses* by making clear what is and is not acceptable behaviour.

Researchers have assessed the extent to which situational crime prevention techniques can be applied to fraud, for example in tackling corruption (Tunley et al, 2018); cybercrime and information security (Hinduja and Kooi, 2013); food fraud (Lord et al, 2017); and different types of organised crime (Bullock et al, 2010; Cornish and Clarke, 2002; Von Lampe, 2011). The key research

insight underlying the application of these techniques to fraud is that offenders admit to viewing fraud as an attractive crime to commit because it is easy to carry out and they are unlikely to get caught (Gill, 2011; 2018; Levi, and Schuchter, 2015). Changing that perception is key.

These studies and others (Button et al, 2016; Levi and Williams, 2013; Wall, 2007) have emphasised the role played by national and local stakeholders other than the police in implementing effective prevention measures. The police role is therefore one of a partner, helping to educate by raising awareness, and encouraging good practices so that offenders, as one local Economic Crime Team investigator noted, come to believe *"this isn't an easy option anymore"*.

As we shall see below, many of the methods currently being deployed to prevent fraud build, even if implicitly, on these theoretical insights.

5.2 NATIONAL FRAUD PREVENTION ACTIVITY

National strategy and organisations involved in fraud prevention

The government's national crime prevention strategy is detailed in the Home Office's *Modern Crime Prevention Strategy* published in March 2016. This outlines the role of prevention in targeting six main drivers of crime[67] and while fraud and cybercrime are viewed as preventable (Home Office, 2016a), the strategy does not go into detail about how this will be achieved.

Fraud is also seen by the government and the law enforcement agencies as falling within the scope of its serious and organised crime strategy (HM Government, 2013). Our previous research lends credibility to this focus; we found that up to 45 per cent of recorded fraud meets the government's definition of organised crime, and in reality the figure is likely to be higher (Crocker et al, 2017). The strategy distinguishes between four different approaches to tackling organised crime, and by extension, fraud, known as 'the 4 P's':

- Pursue: investigating individuals or groups involved in fraud to disrupt their networks and activities and bring offenders to justice.
- Prevent: stopping people getting involved in fraud in the first place and identifying individuals and business who are known to be enablers of fraud.
- Protect: protecting individuals, systems and communities against fraud through crime prevention measures, such as awareness raising and training, and supporting efforts to 'design out' crime.
- Prepare: reducing the impact of fraud where it does occur by working with others to better understand how it occurs in the first place.

It is notable that some counter-fraud professionals we interviewed in the police often framed their thinking about fraud prevention with reference to 'the 4Ps', as demonstrated in the comment from a specialist in the City of London Police:

> *'The police are generally reactive … for fraud we're trying to massively increase the Protect and the Prepare approach.'*

There are multiple national actors involved in delivering fraud prevention work (for example, see National Audit Office, 2017). The government plays a key role, with the Joint Fraud Taskforce coordinating a strategic response across a range of public and private sector bodies. The City of London Police delivers targeted awareness raising campaigns and the National Crime Agency coordinate's work with multiple fraud agencies and regulators as well as the private sector to ensure they are taking action to prevent fraud (the newly established National Economic Crime Centre is soon to take a role which as yet is undefined[68]). There are in addition many organisations with a focus on discrete elements of fraud such as the National Trading Standards team, who work to prevent scams perpetrated by mass-marketing (especially postal) and doorstep fraud.

Alongside these bodies, others take the lead on preventing cybercrime, which as we discussed in Chapter 2, incorporates many fraud offences and is an enabler of them. These include the National Cyber Security Centre which identifies and targets emerging cyber-dependent threats and coordinates a regional to local response and the National Cyber Crime Unit in the NCA. The government runs awareness raising campaigns and in partnership with the private sector, the Get Safe Online campaign to help raise public awareness of online protection.

In addition organisations in the private and the third sectors play a significant role in preventing fraud. Key strands of the private sector response include the

[67] These are identified as opportunity, character, the effect of the criminal justice system, profit, drugs and alcohol.

[68] For example, see http://www.nationalcrimeagency.gov.uk/news/1257-national-economic-crime-centre-announced [accessed 24.08.2018].

development and implementation of security solutions to prevent fraud targeting systems, products or services, flagging and preventing risk (particularly in financial services) and raising the awareness of those who use their services. Cifas also manages a database of previous victims who register, as well as vulnerable people[69], and alerts member bodies if product applications are made using their details to prevent fraud. The third sector produces and disseminates a considerable amount of fraud prevention material, with organisations such as Citizens Advice, Age Concern, Fraud Advisory Panel, Finance UK and Cifas playing a key role.

Education and awareness campaigns

Much fraud prevention work in the UK from the public and private sector has focused on raising the public's awareness of risk so that people and organisations can better protect themselves. These campaigns make use of many of the crime prevention principles set out above, aiming to change the attitudes and behaviour of the public to increase the effort for offenders and to reduce the rewards. We sought to identify the most significant education and awareness raising activities undertaken nationally, regionally or locally to target fraud.

Tables 12-14 set out a wide range of initiatives that are aimed at:

- The general public as a whole (Table 12).
- Groups that are known to be susceptible to fraud or related cybercrime, or (Table 13).
- Raising awareness of a specific scam. (Table 14).

TABLE 12: Education and awareness campaigns aimed at the general public as a whole.

Project/Campaign	Examples of work
Get Safe Online (joint government/private sector)	Initiative to tackle volume internet crime nationally and locally.
Financial Fraud Action UK (part of UK Finance)	Coordinates crime prevention for the financial services industry. Led on the 'Take Five Campaign' with other partners. Offers simple and practical advice to the public and organisations to help protect against financial fraud, specifically in relation to 'scams' or social engineering frauds.
Scams Awareness (Citizens Advice)	Runs annual Scam Awareness Month campaigns.
Cyber Aware (HM Government) (formerly Cyber Streetwise)	Aim to encourage the public and small businesses to adopt simple and secure online behaviours
Cyber Essentials (National Cyber Security Centre)	Certification system to give protection against the most common cyber-attacks.
Fraud Advisory Panel	Produces guidance, research and training for individuals and organisations on a range of fraud topics.
Cifas	Provides awareness raising campaigns, in particular to tackle identity and related fraud.
Crimestoppers	Runs campaigns to educate the public and organisations about fraud. Recent campaigns include 'Game of Fraud'.

[69] As defined by the Mental Capacity Act 2005.

TABLE 13: Education and awareness campaigns aimed at specific groups.

Project/Campaign	Examples of work
Cyber Protect (Regional Organised Crime Units and police)	Police programme to safeguard the public and businesses from cybercrime.
Initiatives targeting the elderly population such as Age UK and Outreach Solutions	Age UK provide information and advice, on how to spot and avoid scams. Outreach solutions is a non-profit organisation that has a programme called *Tackling Fraud Together 2020* and develops fraud prevention messages using existing structures and services (such as those of Age UK and Rural Action Community Group).
Victim services	Generic advice and support to victims who report crimes and accept the support.
National Business Crime Centre	Supports businesses to navigate their way around police force structures and priorities. Some work to raise awareness of fraudulent activities and flag patterns of offending which typically has a wider crime prevention focus.
Cifas and Financial Fraud Action UK	Ran *Don't Be Fooled* campaign to deter young people from becoming money mules, including lesson plans for delivery in schools.
Safer London	Works with young people, including providing education and training for keeping safe online and to help young people to avoid getting involved in criminal activities.

TABLE 14: Fraud alerts. [70]

Project/Campaign	Description of work
Action Fraud Alerts	Email sign up for local scam information and other publicised alerts.
Cifas	Send out fraud alerts to members.
Fraud Forums	Regular fraud updates to members
Cyber Security Information Sharing Partnership (CiSP) – membership scheme for businesses	The National Cyber Security Centre issue alerts and advisories to address cyber-security issues being detected in the UK as well information-sharing between member organisations.
UK Finance	Sends out scam alerts to leading firms providing finance, banking, markets and payments-related services in or from the UK.
Organisations with customers (eg banks)	Email and online alerts to customers.

[70] These tend to be more in use for tackling fraud and cybercrime against businesses and are more a reactive approach to crime reduction, raising awareness and vigilance in real-time as a particular crime series reveals itself.

As these tables demonstrate, there are many education and awareness campaigns aimed at either the public as a whole or at specific groups. However responses in our interviews and surveys highlighted concerns about the impact of this activity. First, there is some evidence from our research that the multiplicity of actors and initiatives may be undermining the potential benefits. Interviewees thought that the cluttered and overly-detailed fraud narratives from an array of different sources did not equip those at risk with the knowledge to identify and avoid fraud (Cross and Kelly, 2016a). This was also a key finding from a government review of the response to online fraud (National Audit Office, 2017 [71]):

> *'There is a lack of coordination and consistency in education campaigns to improve citizens' and businesses' cyber security.'*

Senior policymakers suggested that the message needed to be simplified in order to have impact. The following comments were given by a senior strategic lead in the police and a business representative:

> *'There are lots of prevention campaigns but my concern is that they confuse people ... it all becomes a bit complicated.'*

> *'A small business doesn't really go around making all these subtle differentiations... all these voices, it's quite a confused landscape and what we think is that there doesn't need to be more of it there needs to be less of it … there's not one voice raising awareness in a really substantial and coherent way.'*

There is a need for much greater national coordination of this work. Due to its national perspective and remit and its role in bringing together the public and private sector stakeholders The Joint Fraud Task Force, would be well placed to take on responsibility for coordinating fraud prevention advice across the public, private and third sector.

Recommendation 14: The Joint Fraud Task Force should coordinate and consolidate the messaging from fraud awareness campaigns delivered across the public and private sector.

Second, there is a lack of evidence about 'what works' in terms of fraud prevention messaging. There is some evidence that the public are overwhelmed with excessive information (so-called 'white noise') which they are unable to assimilate (Cross and Kelly 2016a). More research is needed to ensure that the messaging from public agencies and other organisations about the risks of fraud and cybercrime is effective.

Recommendation 15: The Home Office should commission research to examine the effectiveness of public awareness campaigns for fraud and cybercrime prevention. The research should produce recommendations for more coordinated and targeted delivery of these communications.

5.3 LOCAL PREVENTATIVE ACTIVITY

Our research identified numerous examples of fraud prevention work carried out by police and local partners, much of which has a focus on relatedcybercrime. A typology with examples is set out in Table 15.

Preventative activity by the local police

Fraud prevention is not a major priority for police forces (Doig and Levi, 2013; Levi, 2008a; 2010). Our analysis of police and crime plans found that, although several highlighted prevention or early intervention they provided limited details about what this would entail. Local strategic partnerships for delivering prevention were either absent or delivered on the basis of fixed-term resourcing.

In our survey of police force strategic leads most claimed to have strategic partnerships in place for delivering preventative work (97 per cent) or disrupting fraud offending (84 per cent). However very few described bespoke local partnership arrangements, with most listing other statutory or national enforcement or support agencies. The most commonly cited partnerships were Trading Standards (19 forces) and Victim Support (nine forces).

Work with victims/prospective victims

What local police activity there is focuses on changing the behaviour of the general public, with an emphasis on those who are assessed as being at high risk of serious and ongoing harm. These are often existing victims who are at risk of repeat victimisation.

The police are well placed to deliver fraud prevention advice, particularly to 'hard to reach' and vulnerable people, because of their local presence. However, there are a number of barriers to them doing so. First, the police resources are under considerable pressure locally and fraud prevention is not a major priority. Recent Police Foundation research has shown neighbourhood policing teams, generally best placed to provide proactive crime prevention advice, have been cut back

[71] National Audit Office (2017) p.8.

TABLE 15: Examples of fraud prevention activities undertaken locally.

Engaging the local public
Local campaigns to raise awareness and enhance personal or business security against fraud. • Distribution of posters and leaflets as part of fraud awareness campaigns – for example, Scam Watch in Derbyshire an initiative which involves multiple organisations, including Citizens Advice, the local council, third sector charity groups for the elderly and the local PCC. • Officers in Durham Economic Crime Team engaged extensively with the local community on social media websites to promote fraud awareness and prevention measures. West Midlands recruited a 'Digital PCSO' who engages with the local public via social media as well as face-to-face visits with community groups. • In Sussex, the Op Signature brand (which is focused on vulnerable victims of fraud) is publicised by neighbourhood policing teams who speak on the subject to local community groups and meetings – for example, Neighbourhood Watch meetings and with banks.
Engaging communities
Delivering seminars, talks or other communications, especially for those who do not think they are at risk of fraud, or for those with limited awareness. • Awareness-raising for older people delivered by a pilot partnership between City of London Police and Age UK in a number of London boroughs. • Volunteers from Avon and Somerset police and in the community in Bristol working to raise awareness among the elderly of relevant fraud-related risks – specifically postal and doorstep fraud. This includes proactive engagement with those at risk and publishing articles to flag awareness among the elderly. • The Metropolitan and Durham police described going into schools and delivering presentations to children. The focus could vary from raising awareness to develop fraud prevention champions in the community, to highlighting the risks of engaging with fraud or cybercrime. • In Kent and Essex a cyber-prevention team aimed to build relationships with the local business community and develop awareness and capability in fraud and cybercrime prevention.
Engaging with fraud enablers
In addition to those at risk of victimisation, engagement may be targeted at others who may fail to acknowledge how their actions are enabling criminality. • Kent Police delivered presentations to students, highlighting the issue of 'money mules' warning them not to allow people to use their bank accounts which may facilitate money laundering. Running campaigns with local taxi firms to raise awareness of anyone picking up a package from an elderly person. • In partnership with the Royal Mail, Trading Standards, seek to identify scam mail and prevent it from being delivered. • West Midlands police delivered light touch intervention in cases where investigation was not viable – commonly young people suspected to have taken the initial steps to purchasing the digital tools or software for perpetrating related cybercrime.
Building local capability, knowledge and awareness
Building up the capability and confidence of local practitioners to identify and act against vulnerability, and improve resilience from within communities. • Trading Standards in the south-west delivering training and awareness raising to the local police and other local frontline practitioners to help them identify and support fraud victims. • A 'Digital PCSO' whose roles were in part to build awareness and capability of colleagues in cybercrime prevention. • Durham engaged with members of the community to encourage them to relay their knowledge to at least two other individuals, thereby raising awareness.
Identify and address vulnerability
Target victims at risk of repeat victimisation. • Local work by Trading Standards to disrupt criminal activity by utilising call-blockers and designating no cold-calling zones. • Local police force working with Trading Standards to reach out to potential victims. • Operation REPEAT (Reinforcing Elderly Persons Education at All Times) in Lincolnshire and Northamptonshire. The programme is working with Trading Standards to safeguard and educate vulnerable adults about doorstep crime and mail fraud. • Essex developed literature and a questionnaire to disseminate to at-risk communities to highlight the dangers of falling victim to scam mail.

and in some forces have ceased to operate in a meaningful way (Higgins, 2018).

Despite the fact that local police forces routinely provide crime prevention advice around traditional crime, the police role in delivering fraud prevention advice is unclear and inconsistent. The presence of local police officers in communities, is not being consistently leveraged to communicate basic fraud and cybercrime prevention messages, representing a missed opportunity.

Recommendation 16: Police officers should to be trained in how to deliver effective fraud and cybercrime prevention messages and local policing teams provide this advice as routinely as they give out other crime prevention messages.

Second, the police generally lack a strategic picture of fraud victimisation locally which inhibits preventative work. Few police forces make use of fraud data and the strategic assessments provided by City of London Police to understand their local fraud problem, and then implement targeted, problem-oriented, prevention initiatives. This means the police know little about local victims, the impact that fraud has had on their lives, the perpetrators and their modus operandi and so ultimately, the specific problem in their locality. A substantive element of the fraud problem will be national in scope, but its distribution and impact within the police force will be influenced by the local social, demographic and economic composition across their communities.

In part this is a product of the way the victims' data and assessments by the City of London Police are compiled: the primary means by which 'problems' are differentiated in these strategic assessments is by National Fraud Intelligence Bureau category codes that reveal little about who the victims are, the manner in which they are victimised or the harm experienced.

It is also because, as we discussed in Chapter 4, our understanding of vulnerability to fraud, and the harm caused by fraud, is not strong. We lack a clear understanding of where the risks in the community are weighted. There has been some attempt to focus crime prevention on groups who are thought to be particularly vulnerable to certain types of fraud, in particular the elderly and those with disabilities. However, even this work, which encapsulates a range of advocate groups in the statutory and third sector, does not seem particularly well coordinated. In our survey of police forces, few described bespoke strategic partnerships in relation to fraud, with most pertaining to Trading Standards, in some cases as a mean of sharing intelligence.

Recommendation 17: The local fraud data provided to police forces by the National Fraud Intelligence Bureau should be presented in a way that helps local police forces understand their specific fraud problems and the characteristics of the victims involved. This will ensure that forces are better placed to develop targeted prevention advice and take a problem solving approach particularly for fraud carried out by local offenders on local victims.

Third, the multiplicity of agencies and actors involved in local preventative work gets in the way of any particular organisation taking action. One Economic Crime Team lead in a local police force commented:

> *'The suckers list*[72] *is Trading Standards owned, not police, one of the barriers to* [the joint operation] *was* [the attitude] *why are we dealing with an initiative that is not the police? … have we not got enough work of our own? Why are we taking on theirs?'*

Police officers in another force told us that there is a lack of clarity and understanding around the role and remit of police forces and Action Fraud. They felt that the responsibility for providing fraud prevention advice should be mainstreamed into the work of ordinary local police officers. Indeed these officers had adopted their own prevention messaging campaign, which is symptomatic of the confusion in this area.

Work with offenders

In addition to work focused on victims, another area that is neglected is preventative work to target and deter fraud offenders locally. Our research has shown that fraud is largely excluded from local four Ps frameworks for delivering a response to serious and organised crime (Garner et al, 2016), which limits the use of intelligence to identify, divert or disrupt local fraud offenders. In our survey of strategic police force leads, many described fraud as a low priority or not applicable in local profile assessments of serious and organised crime (n=20, 62.5 per cent), strategic risk assessments (n=21, 65.6 per cent) and control strategy[73] (n=20, 62.5 per cent). In addition to this hindering wider prevention efforts it also limited the use of intelligence-led enforcement and prevention activity against suspected offenders.

[72] The 'suckers list' denotes the repository of intelligence on suspected victims and is used to direct welfare visits by Trading Standards.

[73] These are annual assessments which assess the array of threats from serious crime and establish where to prioritise police resources.

Turning to the management of convicted fraud offenders in the community, in our survey of strategic police force leads nearly two thirds (n=20, 63 per cent) assessed their response to offender management in fraud as 'satisfactory'. A small number of Economic Crime Team practitioners described examples of prolific fraud offenders who were not being effectively managed following conviction, with limited use of measures to inhibit offending such as Serious Crime Prevention Orders:

> *'… really small financial value*[74]*, really young, absolutely prolific, no remorse about what he'd done … we know someone like that will come time and time again.'*

> *'Whilst, when an offender is identified and, where possible, arrested, the basic offender management is good, there are missed opportunities in respect of applying for orders to control their onward offending* potential.'

The police are inhibited in desistance work by a weak evidence base. There is very little research on what interventions are effective. Recent research into organised crime groups linked to fraud suggests a need for better controls to inhibit the use of enablers in professions (eg solicitors) that are key drivers of serious fraud offending.The research highlighted that this needed to involve a much wider set of bodies than just the police, not least the professional regulators (May and Bhardwa, 2018). At the national level the NCA has focused its desistance efforts on the perpetrators of cyber-dependent crime, with little focus on fraud[75].

Recommendation 18: Serious and persistent fraudsters (including those involved with known organised crime groups), vulnerable groups and victims, as well as emerging systemic vulnerabilities should be incorporated into police profiles of the local serious and organised crime threat. The assessment should be developed collaboratively by the police, local authorities, third sector and local business representatives, and used to support targeted local prevention strategies.

Preventative activity by other local actors

There are many examples of local schemes led by voluntary, public and private organisations.

Taking voluntary sector work first, Citizens Advice plays an important role in providing fraud prevention advice. The Citizens Advice national campaign team said that the best Citizens Advice offices work with partners (such as local authorities or Age Concern) on individual issues, especially in relation to mass mailing scams. Whether it was on their agenda depended somewhat upon the interest of the staff, local priorities and whether they could get funding to carry it out, usually from local authorities and PCCs. Data is provided to the Citizens Advice central office and sometimes this sparks an interest, including how many calls about specific scams they are receiving in different localities. But focus and attitude varied between local offices. Often this was down to the relationship with other providers, such as Trading Standards. As one member of the national campaigns team said:

> *'… some work together exceptionally well and some don't even talk to each other.'*

In relation to scams and frauds, the more proactive Citizens Advice offices usually network and engage with others through bodies such as adult safeguarding partnerships. An example of good practice in partnership working was Op Signature in Sussex, an initiative which is very locally focused and involves multiple organisations, including Sussex County Council, Neighbourhood Watch, Victim Support, Age UK, befriending services and the local PCC.

The public sector agency most central to local fraud prevention work, other than the police, is Trading Standards. The National Trading Standards Scams hub has developed intelligence on members of the public at risk, especially from postal scams. This information is disseminated to the local Trading Standards office for staff members to make contact with potential victims and conduct welfare visits to assess the individuals at risk from fraud. Staff also engage with other local services such as the police or adult social services to establish whether the person is known to more than once agency. However the scale of demand considerably outstrips local resource to deliver what can be intensive engagement and support, with over 30,000 suspected victims referred to local Trading Standards services from when the hub began to January 2016 (Lonsdale et al, 2016). Trading Standards, suffering their own resource constraints, [76] are often unable to deliver:

[74] It should be noted that this small value is described in the context of some of the most high value frauds investigated in the police force by an Economic Crime Team, and in fact related to a fraud-related loss of £20,000.

[75] For example see http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved [Accessed 16.08.2018].

[76] The number of Trading Standards officers has fallen by 56 per cent since 2009 (NAO, 2016).

'[There are] Only two of us doing this work ... [we] need to prioritise by determining [the] level of vulnerability.'

Police force engagement with Trading Standards is variable. One police force was not working with the service at all, and in another a previous initiative to work with Trading Standards (using their local Police and Community Support Officers (PCSOs)) was discontinued due to reductions in local resource, competing demands and challenges in targeting efforts because of inadequate intelligence. A local Trading Standards officer outlined the gaps in partnership working:

'I sit on a Regional Doorstep Crime Group and there is not a police presence any more, it used to be that forces did send representatives, but this no longer happens, meaning our relationship with the police is non-existent.'

A leading public-private sector initiative is the Banking Protocol, which is a national initiative led jointly by the police and the finance sector. Staff in local bank branches are being trained to flag suspected fraud incidents including ones where the offender and victim are present in the bank. The protocol enables bank staff to contact the police if they suspect a fraud is occurring, whereupon the police will respond and intervene where necessary. Figures from UK Finance show that the protocol has prevented the loss of £24.7 million since its introduction and led to 197 arrests (UK Finance, 2018 - press release 22nd June 2018 [77]).

The use of shared financial intelligence between the banks and law enforcement is another means to proactively identify risk and vulnerability (Cross and Blackshaw, 2014). The banking sector typically flags transactions that are of concern as part of the Suspicious Activity Reports (SARs) regime, on the basis of factors such as the customer's age and the circumstances of the transfer (for example if,it is made to a specific country overseas or it is an unusually high amount of money). The volume of intelligence received will vary across the country but Durham police (for example) told us that they receive 'a handful' of reports each day and then task local police officers to visit the victims where there are concerns. However, the use of this intelligence is variable across the country and dependent on the priorities in each local police force, as indicated by a local financial intelligence officer:

'All forces should be using them – some don't use them at all, others have four people in a team looking at SARs.'

We conclude that there is a lack of clarity around roles and responsibilities of different agencies and therefore poor coordination of messaging and effort. Police and Crime Commissioners given their broad crime, policing and (in some cases) fire remit and their responsibilities to victims of crime stand well placed to provide leadership in this space.

Recommendation 19: Police and Crime Commissioners should establish fraud prevention partnerships or at least explicitly include fraud and cyber prevention work within existing local crime prevention partnerships and strategies. The plans developed by these partnerships should be clear about who will be leading on local fraud prevention work, and what this will involve.

Prevention work aimed at business

The newly formed National Business Crime Centre (NBCC), does not have any operational or specific prevention responsibilities relating to fraud (or cybercrime), but it supports businesses by working to raise awareness of fraudulent activities, identifying and flagging patterns of offending and helping businesses navigate complex law enforcement structures. This is important because building up resilience to crime can generally help mitigate all types of risks which includes fraud and cybercrime.

However, there is scepticism among law enforcement professionals about working with the private sector on crime prevention (Gill and Howell, 2017) including a belief that businesses, including very large ones, are complacent about crime generally (Hopkins and Gill, 2017), as well as fraud and in particular about cyber security (Williams, and Levi 2017). One police officer in a Regional Organised Crime Unit Cyber Protect team explained:

'We want board level members of the organisation There is more work to be done in virtually every organisation, ultimately we need to convince [them] that this is an area that requires their attention.'

We were told by practitioners that regional cybercrime teams prefer to work with larger companies of around 100-250 employees, to maximise their reach and to focus on those, who if compromised, would have the most local impact in terms of jobs and resources lost. However even in these large companies they still find basic fraud prevention procedures to be inadequate. One police officer from the Cyber Protect Team

[77] Available at https://www.ukfinance.org.uk/banking-protocol-prevents-25m-in-fraud-and-leads-to-197-arrests/ [Accessed 18.10.2018].

remarked about the readiness of some organisations to counter cyber threats:

> *'The vast majority, outside of very large organisations, it's generally very poor ... they're virtually all not really where they need to be.'*

One particular problem that officers identified was when small companies grow very quickly, their IT systems grow with them, but their level of security does not always catch up. This is often because IT personnel are not experienced enough for this increase in the size of the network. As one police officer warned:

> *'... they've grown, but their awareness and sophistications haven't, we've got some quite big companies and their security is at nursery or primary level.'*

Small businesses can be particularly disadvantaged when it comes to crime prevention due to limited resource to invest in capacity or skills in cyber security thereby leaving them vulnerable to fraud. While they face similar risks to larger corporations they have much smaller budgets to tackle these (Kurpjuhn, 2015; Pritchard, 2010). They are rarely a particular focus of local police attention, however, criminals are increasingly targeting smaller businesses, precisely because they are perceived to have weaker security defences (Renaud, 2016).

The Federation of Small Businesses (Unpublished) has found that their members are taking more security precautions against crime (generally rather than fraud specifically) than ever before but they felt neglected by the police. A representative from the small business community said during our interviews:

> *'Small businesses are very much the "Cinderella group" in relation to crime in general ... all the national initiatives are based around big financial, service firms.* [The Joint Fraud] *Taskforce, has no small businesses presence whatsoever, which I think is a pattern that repeats itself ...* [small business] *tends to be an afterthought, if a thought at all.'*

At the local level, police prevention support locally for businesses varies widely across the country. National protocols for victim support do not take into account businesses of any size, and regardless of this, there are no means to differentiate small from large businesses in the crime data.

As our own research found, most police and crime plans do not reference business crime at all, but where they do, much of their focus is aimed at larger businesses.

A Federation of Small Businesses (FSB) representative described police attention for small businesses in general, as a "void", which also included fraud. They stated:

> *'Locally, it depends on the PCC, but a lot of them don't seem to engage with small businesses at all …. The message you'll get from small businesses is that the relationship with the police isn't particularly great, because they don't seem to care.'*

There is a serious blockage to progress here: on the one hand businesses do not report fraud because they don't see the value, but on the other hand if they don't report it, the police cannot build up a profile of offending on which to determine the best course for a response. Action Fraud stated that it only received 1,073 cyber dependent crime reports from businesses for year ending October 2016. This lack of reporting may take many forms, such as deciding to deal with fraud internally, perhaps for reputational issues, or choosing to take civil action (for discussion of related issues see Walby and Lippert, 2014). As one officer from a Regional Organised Crime Unit Cybercrime team remarked about this issue:

> *'If you were to look at reported cyber-dependent crime, you would think it's not a massive problem ... understandably they're* [business] *a bit twitchy, they don't care who did it, they just want to be back up-and-running again.'*

We conclude that fraud is under-reported, in particular by the private sector. Victims are not encouraged to engage with the authorities due to a lack of clarity about the importance of reporting fraud, the information they need to provide and the action that will be taken after they have reported it. The Joint Fraud Task force is well placed to assist here but remains in its infancy and has not yet managed to engage companies from all relevant sectors. This limits the police intelligence picture on offenders and emerging trends and patterns.

Recommendation 20: Consolidating fraud intelligence data from across the public and private sectors should be an ambition for the government. This would augment current capability to identify offenders, recognise vulnerability and emerging threats and direct public resource to where it is most needed. As a first step there should be a stock-take of information collected by different bodies and an analysis of how these can be effectively integrated and applied to fraud policing.

5.4 SUMMARY

Prevention is rightly seen as the best way to tackle a volume, cross border crime like fraud, of which the pursuit of offenders can only ever be a small part of the effort, relative to the scale of the problem. We have identified a number of promising initiatives around the country, including lots of awareness campaigns and work targeted at some vulnerable groups.

However, we also found major gaps in the effort to prevent fraud. Public awareness and education campaigns are fragmented and the evidence base on their impact is lacking.

Locally, prevention work is poorly led and coordinated. There needs to be a much clearer delineation of roles and responsibilities so that messaging is consistent and the impact of different projects and initiatives adds up to more than the sum of their individual parts. In light of their relationships with local communities, the police could play a stronger role in providing fraud prevention advice but they are unclear about their responsibilities and they lack a data-informed and evidence-based picture of where harm, vulnerability and prolific local offending are located. This in turn obscures how fraud is to be assessed and prioritised against the multitude of other demands on local resource. There are a multitude of organisations and partnership arrangements with a role in fraud prevention but much more coordination is needed to ensure these efforts are targeted effectively.

6. BUILDING A BETTER SYSTEM FOR TACKLING FRAUD

This chapter examines why the shortcomings in the police response to fraud exist and what needs to be done to put them right. While the report has highlighted many examples of good practice, it is clear that overall the response is falling short of where it ought to be if we are to catch or disrupt fraudsters, support victims and prevent fraud in the first place. In the course of this report we have identified a range of problems within three different parts of the response: enforcement, the service provided to victims and prevention. In this chapter we argue that sitting behind these operational failings is a deeper problem: we simply do not prioritise tackling fraud across the UK, and consequently the national law enforcement system we have put in place to tackle it is inadequate.

The chapter focuses on three areas which together make up the main components of the national law enforcement system for tackling fraud:

- *Governance and strategy*: how fraud is situated within wider national and local strategies for tackling crime, the degree to which it is prioritised, relative to other types of crime, and the extent to which actors throughout the system are held to account for their performance in tackling it.
- *Structure*: how the operational response to fraud is organised at national, regional and local levels.
- *Workforce*: who is tasked within law enforcement with tackling fraud and whether they have the capacity and capability to do so effectively.

We conclude that in each of these areas the system is currently inadequate and we make a series of recommendations with the ambition of achieving a step change in our national response to fraud.

Before we begin we ask perhaps the most fundamental strategic question which needs to be addressed before progress can be made: should the police and their partners give fraud greater priority?

6.1 SHOULD WE PRIORITISE FRAUD?

As we shall show below, fraud is not prioritised by the government or by local policing and in many ways this reflects public opinion. The latest survey of public attitudes about policing commissioned by HMICFRS and carried out by Ipsos Mori found that the public typically gave greater priority to other matters than fraud. When asked directly about which different offence types should be among the top three priorities for policing 61 per cent said violent crime, 54 per cent said terrorism/extremism and 49 per cent said rape and other sexual offences, while only four per cent mentioned fraud, fewer than those who mentioned online abuse and drug offences (Ipsos MORI, 2017).

In this context should fraud be more of a priority for the police? Given the range of problems policing and law enforcement agencies are facing and the serious harm they cause (for example child sexual exploitation, modern slavery, sexual crime, domestic abuse, extremism and terrorism), and in the context of recent budget cuts, it is understandable that fraud has not received greater strategic focus.

However, we can accept that difficult context and be realistic about what can be achieved, while also recognising that fraud deserves greater attention from public policy and law enforcement. First, the aggregate harm caused by fraud is considerable. As Button et al (2017) have shown, fraud is estimated to cost the UK £190 billion a year, with £6.8 billion as a result of fraud that directly targeted individuals. The UK loses more financially every year to fraud than for most other types of organised crime (Mills et al, 2013). These are not just real losses to families and businesses, but they also result in funds being channeled out of the UK and into the criminal economy. This aggregate level of harm and financial loss cannot be ignored by responsible policy makers, even if it is much less visible to the public than problems such as burglary and vehicle theft.

Second, preventing and investigating fraud is part of a strategy for dealing with other types of crime. As we have seen, fraud is closely connected with other aspects of organised criminal activity, including most notably cybercrime (and associated identity theft), money laundering, corruption, counterfeiting or illegal supply (May and Bhardwa, 2018), many of which are intrinsic to serious fraud. Many organised crime groups are involved in more than one type of crime. Investigating fraud should not be seen as a distraction from the fight against serious and organised crime, but rather a core component of it.

Third, although the relationship between fraud and vulnerability is not fully understood by researchers or law enforcement, there is evidence that vulnerable groups are being targeted and many such individuals become repeat victims. A significant minority of victims in our analysis of police data reported a high personal impact as a result of the fraud, being a prior victim or a regular target. The harms caused are not merely financial, although those alone can in some cases be considerable, but also involve serious financial exploitation or abuse and psychological and emotional distress (Age UK, 2015; Cross et al, 2016b; Whitty and Buchanan, 2015). It is imperative that vulnerable individuals, many of whom do not report fraud and suffer in isolation, are provided with the protection of the law.

We are not naive about the resource pressures on policing and law enforcement. Indeed, as part of our recommendations below, we argue that there are structural and workforce reforms that should improve efficiency as well as effectiveness. Having said that, if the government wants to see a step change in the ability of law enforcement to investigate fraud more effectively, as well as prevent it and provide a better service to victims, it will inevitably have to invest more money in order to do so.

Why is fraud not a policing priority for the public?

Reflecting on what we have learned in undertaking this research we would suggest that fraud is not a priority for the public for the following reasons:

- Local public opinion tends to focus more on visible crime in public spaces, whereas much fraud takes place online or otherwise in private spaces.
- Not all in the public or business communities perceive the risks online in the same way as in the physical world.
- Financial loss falls overwhelmingly on to the private sector which often takes ownership of the crime in addition to being the victim of it.
- For many, the primary objective is recovery of lost money, not to invoke a criminal justice response.
- There is a crowded ecosystem of public and private sector response services in which the police are not necessarily the most capable guardian.
- Will it make a difference? Too little is done to demonstrate to victims that reporting fraud will generate an outcome.

6.2 GOVERNANCE AND STRATEGY

National strategy

Fraud is the most pervasive crime in the UK, affecting over three million people a year, and yet there is no national strategy for dealing with it. The last national strategy for tackling fraud was published in 2011 by an agency that no longer exists (National Fraud Strategic Authority, 2011) and we found few practitioners at any level made reference to it. Instead, strategic direction is derived to some extent from the Modern Crime Prevention Strategy (Home Office, 2016a), but more prominently from broader strategies to tackle serious and organised crime (HM Government, 2013) where other problems with a higher profile and stronger intelligence base (for example, drug offences) gain greater priority and attract more resources (Crocker et al, 2017; Levi and Maguire, 2012).

More recently there has been a greater national strategic focus on cybercrime. There is now a national agency, the National Cyber Security Centre, which helps to coordinate efforts to improve cyber security. Cybercrime is also a major area of operational focus, with its own directorate in the National Crime Agency. As we show below at the regional level, within the Regional Organised Crime Units, there is much greater focus on tackling cybercrime than on fraud. Of course cybercrime and fraud are linked and so tackling cyber dependent crimes should also help in the fight against cyber enabled fraud. However these connections are not well understood empirically and are poorly articulated strategically. The result is that fraud is 'crowded out' by other connected but competing areas of national strategic focus. As the head of a police Economic Crime Team pointed out:

> *'All* [senior staff] *say is "the* [the City of London Police] *are dealing with that" – fraud sits under the Serious Crime Directorate but is the poor diner at the table. It's only the overlap with cybercrime has meant it's become less of a 'poor diner' but* [it's] *still 'seen as the lesser crime.'*

The absence of a national strategy for tackling fraud is a glaring omission that acts to demobilise efforts to tackle this substantive area of crime. We recommend that the government produces a national strategy for fraud, covering the full spectrum of the four 'P's' with an emphasis on prevention, enforcement and victim services. The responsibility for overseeing the implementation of this strategy should rest with the Home Office. The City of London Police, the lead police force for fraud, should produce a national fraud policing strategy that is located within wider government strategy.

TABLE 16: Perceived priority of fraud compared to other crimes under different assessments. [78]

	High or very high priority	%	Low priority	%	N/A	%
Strategic risk assessment	11	34%	16	50%	5	16%
Control strategy	12	38%	15	47%	5	15%
Serious/organised crime local profile	12	38%	15	47%	5	15%
Police and Crime Plan	9	28%	20	63%	3	9%

Recommendation 21: The government should produce a national, cross-departmental strategy for tackling fraud alongside a specific national fraud policing strategy.

Accountability

This absence of a national strategic focus on fraud means there is weak accountability, throughout the system, for tackling this important area of economic crime. First, accountability among the national agencies is dispersed and confused. The National Crime Agency does not work directly on fraud and is not responsible for the operational response even though it does have responsibility for serious and organised crime which is acknowledged to include fraud. The Joint Fraud Taskforce has been established to coordinate work between the government, law enforcement and industry. The City of London Police is the national lead police force for fraud and is accountable to the government and parliament for the police element of the response. However, the operational policing response is a local responsibility and the City of London Police has no power to hold local policing to account for its performance in tackling fraud.

Second, fraud is not prioritised by the accountability bodies at the local level. Although our review of Police and Crime Commissioners' Police and Crime Plans found that fraud was referenced in 32 of the 43 forces (74 per cent), this still means a quarter (11) failed to mention fraud in any way. Moreover, the type of emphasis given in these plans varied, with some merely mentioning fraud in the context of the Strategic Policing Requirement and others highlighting key areas they intended to focus on such as doorstep fraud or scam victims. Cybercrime and vulnerability received coverage in all PCC plans but often with no explicit reference to fraud. Fewer than half included a reference to vulnerability in the context of fraud (n=18, 42 per cent).

Our research also included our own national survey of police forces to which 32 forces responded. We found that fraud did not feature in a number of key strategic assessments which have a particular focus on serious and organised crime and which help to steer local resourcing and priorities. As Table 16 above shows, in each of the local assessments fraud is considered by most respondents to be a low priority.

When elected Police and Crime Commissioners were introduced, the government recognised the danger of parochialism. The fear was that elected figures would understandably focus on the local matters that tend to be prioritised by voters rather than issues such as cross border crime which might have less visibility in local communities. For this reason the government introduced the Strategic Policing Requirement which sets out the key national threats for local police forces to maintain a readiness to respond to and where necessary, cooperate with other police forces or agencies to do so (Home Office, 2015). The Strategic Policing Requirement does mention the need to tackle *'large-scale and high-volume fraud and other financial crimes'* as these relate to serious and organised crime, but this is an ambiguous reference and the Strategic Policing Requirement says nothing of any substance about what the local fraud response needs to look like nor what the local remit should be for addressing it.

To strengthen accountability, greater clarity is required about who is responsible for what and to whom. The development of a national fraud strategy should be

[78] One caveat is that due to an administrative error there is an omission of a middle response option from the question. Respondents were provided with the option of 'Very High, High, Low or Not applicable'.

accompanied by a clearer allocation of roles and responsibilities. The government should be responsible to parliament for the delivery of this strategy and the City of London Police should report to the Home Office on the implementation of a complementing national fraud policing strategy.

To tackle the weakness of local accountability, the Strategic Policing Requirement should make much more explicit the roles and responsibilities of local forces in tackling fraud and other types of cross border crime . This currently rather brief document should be much clearer about what the government expects from local policing across the board. The fact that HMICFRS is currently carrying out a thematic inspection is positive and should be followed by much more regular scrutiny of forces' performance on fraud (regionally and locally) through the PEEL framework.

Recommendation 22: The Home Office should be responsible for overseeing the implementation of the national fraud strategy. The City of London Police should be responsible for ensuring delivery of the national fraud policing strategy.

Recommendation 23: The Strategic Policing Requirement should be much more explicit about how local forces are expected to approach fraud and cross border crime generally. HMICFRS should inspect against this expectation.

Performance management

Given the low prioritisation of fraud politically at both national and local levels it is not surprising that we find major gaps in the performance management architecture in relation to this area of crime.

First, police forces do not monitor and record the outcomes of fraud investigations in a consistent way. It is therefore not possible to know whether these statistics are a true representation of effectiveness or simply reflect absent data in some cases.

Second, there is currently little in the official statistics to differentiate frauds on the basis of complexity, seriousness or harm. This makes it hard to come to judgments as to whether forces are using their resources in an efficient and effective way. To draw a parallel with other areas of crime, if a police force were to detect the majority of its shoplifting offences, but none of its aggravated burglaries, they would not be viewed as effective in tackling acquisitive crime.

Third, forces are still arguably measuring the wrong things. In our interviews and surveys police leaders emphasised the importance of prevention as opposed to enforcement in tackling fraud. It is striking that, notwithstanding the difficulties of measuring the effectiveness of preventative measures, there is very little data collected to measure the scope, implementation or effectiveness of prevention work in relation to fraud. The same can be said of the services provided to victims. Even within the 'pursue' strand there is no systematic measurement of disruption activity. So, even though practitioners stress that traditional criminal justice outcomes should not be the singular focus, effectiveness is still largely measured by those very outcomes.

Fourth, until recently fraud has rarely been a key focus of independent inspections of police forces. That said, some work by HMIC (FRS) in the context of wider digital crime revealed differential and inadequate treatment of victims when compared with more conventional crime (HMIC, 2015). The forthcoming HMICFRS thematic inspection will help to address this and should help to shine light on performance in relation to fraud.

Fifth, the police share responsibility for tackling fraud with an expansive web of statutory, private and third sector organisations (see, Button et al 2016), but there is very little measurement of, and accountability for, their response to fraud. For example, there has been criticism of the service provided to victims by banks and there has been criticism of a lack of investment in security and customer awareness across business (Financial Ombudsman, 2015; National Audit Office, 2017). Similarly the governance arrangements among partners in the Joint Fraud Taskforce is unclear, indicated in part by the lack of clear objectives or measures to demonstrate the progress being made in tackling fraud (National Audit Office, 2017).

As strategic police practitioners made clear, all of this adds up to a lack of performance management in relation to fraud:

> *'There are things they know they have to do and things they would like to do and fraud is currently in the like-to-do as there is no performance requirement at the moment …* [it's] *not even on the [performance] dashboard in some forces.'*

> *'Fraud investigations are not subject to the performance management regime that other crimes are given that we do not necessarily own the crime.'*

To strengthen the performance management regime in relation to fraud, we make the following recommendations.

Recommendation 24: Forces and regional units should be required to report back to the National

Fraud Intelligence Bureau not just on criminal justice outcomes but also on victims services, prevention work and disruption activity.

Recommendation 25: The Joint Fraud Taskforce should agree on how the performance of the private sector and other partners will be measured in relation to fraud and then report annually on those measures.

6.3 STRUCTURE

Fraud presents a major challenge to the way in which policing and law enforcement is structured in England and Wales. It is a cross-border crime being dealt with by a fragmented and localised police service. Centralised reporting and analysis through Action Fraud and the National Fraud Intelligence Bureau (NFIB) is vital to gaining a national perspective on a cross border crime. However, currently this means that the understanding of the problem is divorced from the operational response. Both need to be brought together via a reallocation of roles and responsibilities. Below we outline the problems with the way the response to fraud is currently structured.

The national reporting and intelligence hub

The introduction of Action Fraud as a single reporting gateway for fraud, accompanied by a national intelligence centre in the form of the NFIB, has brought a number of benefits. The first is more robust crime recording practices to improve consistency and integrity in decision-making. Previously, police forces were found to apply variable criteria for screening cases and ruling out investigations that were deemed to be lower priority (Gannon and Doig, 2010). Having a single hub means that decision-making is fairer, more rational and more consistent.

Second, the scale and geographic scope of fraud-related criminality has generated large quantities of data which has enabled and necessitated the use of analytics to draw links between victims and offenders and develop a comprehensive intelligence picture. Using a central 'funnel' for most fraud reported by individual victims enables the NFIB to build a stronger analytical picture of fraud offending across the country and improve the prospects of tackling cross-border offenders.

Third, Action Fraud provides a hub to engage and share data with key national bodies in the private sector that are themselves key reporting points for fraud. These include Cifas and Finance UK.

However, the introduction of centralised reporting has separated those with responsibility for understanding the fraud problem (Action Fraud and the NFIB) from those with operational responsibility for tackling it (mainly local policing). This break in the system manifests itself in a number of ways.

First, it has encouraged local police forces to offload responsibility for fraud victims onto Action Fraud. Responsibility for handling crime in the world of policing is generally based on victim location or where the crime is reported. In the case of fraud, the NFIB within the City of London Police (the national crime recording centre) ostensibly has responsibility for the 'crime' as it is administrated but not the operational response to investigate or support victims.

Second, the crime data collected by Action Fraud from victims and assessed by NFIB lacks a focus on harm or vulnerability which limits its traction with local policing. The City of London Police analyses the data it receives via Action Fraud and makes preliminary desktop enquiries to inform the decision to allocate an investigation, almost singularly, on the basis of whether there is opportunity to investigate (for example, an identified offender or other identifier such as bank account number). Crucially the lead force does not differentiate cases on the basis of threat or harm. This generates a downward flow of work that is divorced from considerations within local policing which are generally based on considerations of 'threat, harm, risk and vulnerability'. This creates an inefficient two-tier assessment process, in which time is first invested to determine enforcement opportunity, followed by a second-tier guided in some cases by a repeat assessment of viability, but also by any number of principles that will vary depending on the frameworks adopted in each police force – for example, financial value, the vulnerability of the victim or the local presence of victim and offender.

Finally, the fragmentation of information systems creates barriers to proper assessment and prioritisation. The City of London Police houses data on recorded fraud, whereas the local police possess much of the contextual data in relation to victim, offender, community or non-police partner involvement (eg housing or social services). Neither are integrated and assessments are commonly made singularly on the basis of the information collected by Action Fraud. In our national survey 14 out of 31 police forces reported having no specific analytical capacity for assessing fraud.

To summarise, while there are undoubtedly benefits to having a central reporting hub, the current system has separated those with responsibility for understanding the problem from those with responsibility for tackling it in local policing. Some of this can be tackled by implementing the recommendations made earlier in this

report, such as using more consistent protocols and shared standards across the service. However there is a need to go further and reallocate roles and responsibilities so that we achieve a more focused and cohesive network for tackling fraud with roles more closely matching capabilities.

National and regional specialist resource

Fraud is a cross border crime but the vast majority of its investigation does not fall under the remit of the national and regional bodies and structures responsible for tackling cross border crime. The National Crime Agency (NCA) is responsible for tackling serious and organised crime and while this includes economic crime in general, interviews with practitioners revealed they had limited specific operational responsibility for tackling fraud. Indeed insofar as its work relates to fraud it often does so indirectly through work in adjacent areas such as serious money laundering and cybercrime (National Crime Agency, 2018). This is despite the fact that, as our previous research has shown, up to 45 per cent of fraud meets the government's criteria for organised crime (Garner et al, 2016).

The new National Economic Crime Centre, a multi-agency unit based in the NCA, is intended to help fill this gap but its focus will be on coordinating and tasking efforts to tackle the serious and complex fraud rather than the volume fraud that currently sits within local policing.

The City of London Police houses the national enforcement unit that takes on some of the most serious and complex fraud investigations. It has limited capacity but has difficulty in getting police or agencies to take ownership of identified organised crime groups. The force also delivers national enforcement, funded by and in partnership with the insurance, cards and banking sector; the Dedicated Card and Payment Crime Unit and the Insurance Fraud Enforcement Department.

There is no single national body which sets out for the public or stakeholders what the problem looks like, what the police objectives are, what is being done and the value of this activity. The National Crime Agency and the City of London Police publish annual reviews (City of London Police, 2017; National Crime Agency, 2018) but neither has oversight of the shape and state of the totality of the response but rather specific elements of it (police enforcement and serious and organised crime). This is why we have recommended that the government produces a national fraud strategy and that the City of London Police produces a national fraud policing strategy and is accountable to ministers for its delivery.

At the regional level, the fight against serious and organised crime is led by the Regional Organised Crime Units. Resources are allocated here via the organised crime group mapping framework, but fraud is commonly excluded from this and hence denied access to an important gateway for specialist resource.

Our research also identified an operational rift between the work undertaken to tackle cyber-dependent crime and cyber-enabled (or online) crime like fraud - with the latter being excluded from the growing specialist resource for tackling cybercrime – locally, regionally and nationally. This clearly has a major impact on the amount of specialist resource dedicated to tackling fraud.

In some Regional Organised Crime Units notional fraud investigation teams were observed to have been subsumed by their cybercrime counterparts, adopting more of an ancillary role to the cyber response, instead of one focused on fraud. The result is that fraud committed through cyber enabled means is receiving insufficient attention. This point is illustrated by a practitioner in the NCA who described the growing problem of mandate fraud that uses social engineering to defraud people and therefore, was out of scope for them:

> *'There is no current mechanism for the National Cyber Crime Unit to investigate business email compromise fraud … It's a significant issue currently for companies, but it doesn't fit currently with our structures* [because it is not a cyber-dependent crime]*'.*

Our survey of police strategic leads found that in 24 out of 32 police force areas cybercrime teams dealt with few or no fraud cases. This means the weight of the response regarding cyber enabled fraud falls on local police teams, who as we have seen, are struggling to deal with it.

The operational rift between cyber dependent crime and fraud has a number of causes. At one level it is about a lack of clarity from the data about the relationship between cybercrime and fraud. So, for example, we do not know how much cyber dependent crime is a precursor or gateway to fraud. Nor does the recorded crime data say much about fraud that is carried out via the abuse of online spaces, such as mass-marketing fraud.

But this rift is also the result of cyber dependent crime being prioritised nationally in a way that fraud is not, with the result that only limited specialist capability is being focused on fraud. Our recommendation, above, to have a national strategy for fraud, owned by ministers and the Home Office. is intended to address these national strategic gaps.

Local police forces

With little specialist resource dedicated to tackling fraud, the weight of the operational response falls to local policing. This is problematic because fraud is mostly committed remotely and therefore breaks the standard relationship in investigative work between victims, offenders and location. This affects both the support offered to victims and the pursuit of offenders.

First, victims are poorly served because their case is handled by a force other than their own. The consequence has been to exclude the majority of fraud victims from receiving or being offered any kind of service, and a systemic failure to identify and support those with particular needs. One local member of police staff described the following:

> *'There is no process for dealing with a vulnerability because the crime's not in* [our police force] *…*[we are] *not tasked at the moment to deal with victims for a crime in another area.'*

Nor are victims' local forces tasked with offering them a service. In our national survey just under a third of police force areas said they did not offer any service to their local victims, with some describing no requirement for them to do so or a lack of resource.

Second, the lack of a local victim means that fraud investigations are not prioritised. Without a link to a local victim to whom the police force is in any direct sense 'accountable' it is hard for these investigations to gain traction operationally.

Local police forces, that enjoy closer relationships with their local communities than national or regional units, could have a valuable role to play in tackling fraud We will demonstrate below how most fraud investigations do not require a local presence. What local policing can offer is an immediate response where a report is treated as a call for service, such as where a victim is vulnerable or an offender seems to be local. Forces also have ability to provide fraud prevention advice, as they routinely do with other types of crime. They can also provide a service to those victims identified as vulnerable (referred by an expanded Economic Crime Victim Care Unit) and to whom they can provide a phone call or a safe and well check.

Recommendation 26: The way in which the police response to fraud is structured needs to change:

- ***Nationally the City of London Police should continue to provide the central reporting hub (Action Fraud) and the national intelligence centre (the National Fraud Intelligence Bureau);***
- ***Fraud investigations should no longer be the responsibility of local police forces and all investigations should be handled by regional fraud investigation units that would exist alongside the Regional Organised Crime Units. This network of regional units should be coordinated and tasked by the City of London Police as the lead force accountable to the Home Office. Where the fraud is assessed as serious or complex it should be escalated into the National Economic Crime Centre within the NCA for national tasking;***
- ***There should be a national service for vulnerable victims through an expanded Economic Crime Victims Care Unit (ECVCU), which can then make referrals into local services.;***
- ***Local policing should be responsible for responding to local frauds treated as a call for service, providing local fraud prevention advice and contacting and supporting vulnerable victims in their areas who are referred via the ECVCU.***

6.4 WORKFORCE

A third core component of the national law enforcement system for tackling fraud is the police workforce. Below we assess the degree to which the existing workforce has the capacity or capability to tackle fraud effectively, looking first at the specialist fraud teams and then at the wider police workforce which as we shall see play a major role.

Specialist teams

Previous research has used investment in specialist Economic Crime Teams (ECTs) as a barometer for the level of police commitment to tackling fraud (see Button et al, 2014b; Doig and Levi, 2013).

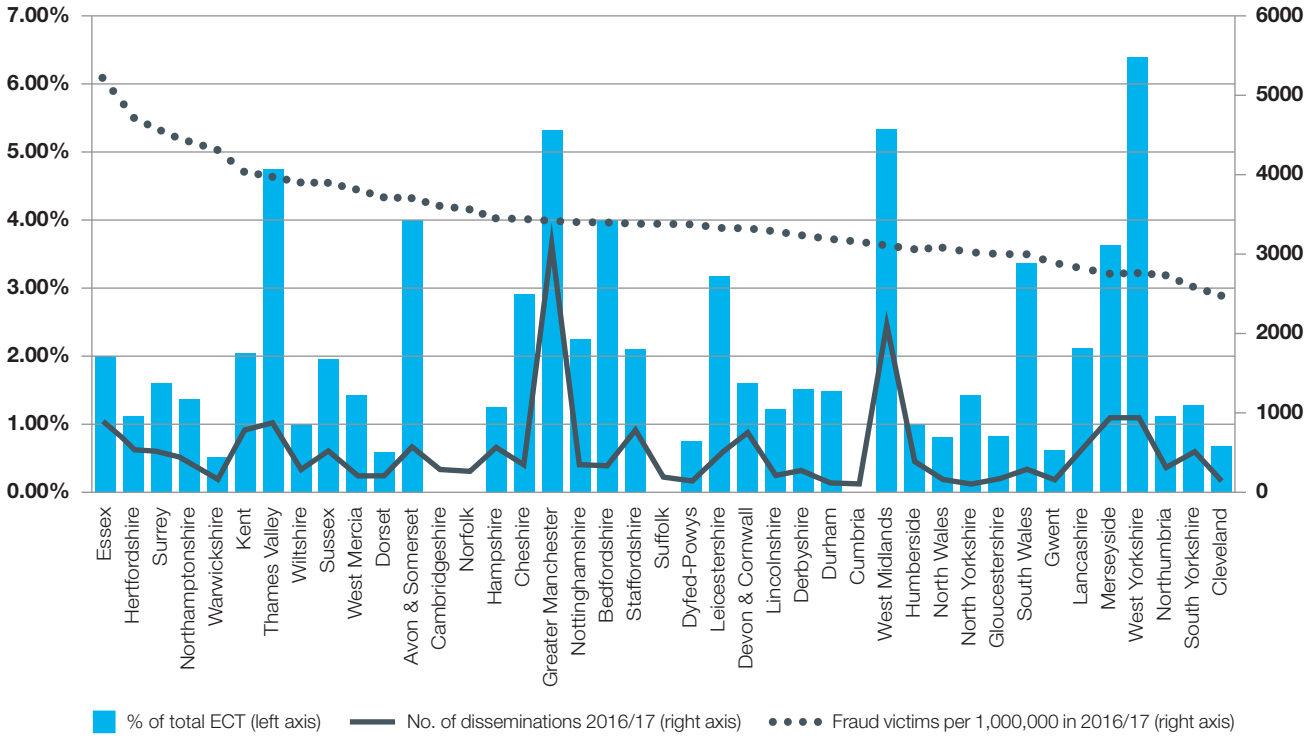
Our analysis shows that in 2017 there were 1,455 (0.8 per cent) full-time equivalent police personnel working in ECTs across England and Wales, nearly half of which were civilian staff (n=667, 45.8 per cent) [79]. This is higher than the number found in 2014 (Button et al, 2014b). It should be noted however that ECTs have a remit beyond fraud, that incorporates financial investigation teams [80] to deal with money laundering and asset recovery in relation to all crime (Howell et al, 2013).

Previous research found over a third of ECT resources consisted of financial investigators (Button et al, 2014b)

[79] Data taken from https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2017.

[80] Financial investigation teams can have a role in developing intelligence, evidence gathering and asset recovery in all aspects of organised and other crime, including money laundering, drug supply and acquisitive crime (Brown et al, 2012).

FIGURE 22: Proportion of police workforce comprised of Economic Crime staff, by proportion of victims and investigations recorded by the National Fraud Intelligence Bureau, 2016-17.



and a survey of 19 police forces revealed that only one ECT considered investigating fraud to be a primary function (Gannon and Doig, 2010). This is reflected in our research with, for example, Avon and Somerset had 58 ECT members recorded in official records, while only eight were described as being dedicated to fraud investigation.

The proportion of staff recruited into ECT functions is inconsistent across the police service, ranging from 2.9 per cent in Bedfordshire to 0.3 per cent in Northumbria, or no ECT at all in a number of police forces [81]. Those without ECTs either refer cases to their regional economic crime teams or may in some cases operate in collaboration with other police forces. Figure 22 examines this composition in relation to volumes of victims in each police force in 2016-17 [82]. Fraud victimisation rates are broadly consistent across police force areas and unsurprisingly, there is little relationship between these and the size of ECTs, as many incidents either do not get allocated for criminal investigation or are allocated to external police forces or agencies for investigation.

There is considerable variability in the size of ECTs when viewed against allocated fraud investigations. In the case of urban police forces such as the Greater Manchester and West Midlands police there is some indication of ECT resource distribution reflecting the number of allocated fraud investigations. Yet, while the number of allocated investigations in West Yorkshire (n=936) and Essex (n=874) is comparable, the former had 6.4 per cent of its workforce dedicated to specialist economic crime while the latter had just two per cent. [83]

Figure 22 indicates that in many police force areas the workload in the form of fraud investigation has little bearing on resourcing decisions for specialists in the ECT. These decisions are likely to reflect the degree of strategic prioritisation of not only fraud but wider economic crime investigation against all other demands.

The degree to which a national resource of 1,455 is adequate for dealing with this volume of fraud investigations (n=36,798) is dependent on a range of factors, not least the amount and complexity of the investigations allocated and the resource expenditure required to deal with them. Interviewees commonly suggested that the existing investigative resource capacity is small compared to the scale of fraud and the resource requirement for responding. This is not a

[81] Not including City of London Police which as the national lead force constitutes a substantive outlier (24.4%)

[82] This chart does not reflect locally allotted investigation (ie police contact treated as a call for service).

[83] The Metropolitan Police was excluded from Figure 22 as it represents an outlier in terms of both case allocation and resource; the force received just under a third (n= 11,605, 30.4%) of allocated investigations and has a fifth of Economic Crime Team resource across the police service (19.4%).

surprising finding. This was particularly true for specialist teams dealing with the most complex cases. For example, one member of a regional fraud team stated that just two investigations would be likely to put his team at capacity. This echoed the following from a strategic police lead for fraud:

> *'The Fraud Team are highly skilled and passionate about investigating Fraud. The problem is that they have a limited capacity and therefore can only accept ownership of cases which are very complex and require their specialist skills. Even then given that we have only five investigators … within this team there is a limit to how many serious/complex investigations they can carry.'*

Our analysis of fraud cases allocated to police forces in the first six month of 2016-17 shows over two-fifths (43 per cent) of cases that reach a positive outcome [84] had taken over six months to complete, with a minority exceeding a year (four per cent). In contrast one in ten cases (9.6 per cent) were resolved within a month (see Table 6 in Chapter 3). This indicates a wide range of complexity but also a substantial number of complex cases that take up considerable resource.

Therefore, within specialist teams the main problem is capacity rather than capability. However there is a concern about the recruitment and retention of fraud specialists. A third (32 per cent) of police force leads reported they were not confident they could recruit the right staff to tackle fraud and a quarter (25 per cent) were not confident in being able to retain them. This problem is especially acute in the most specialist units:

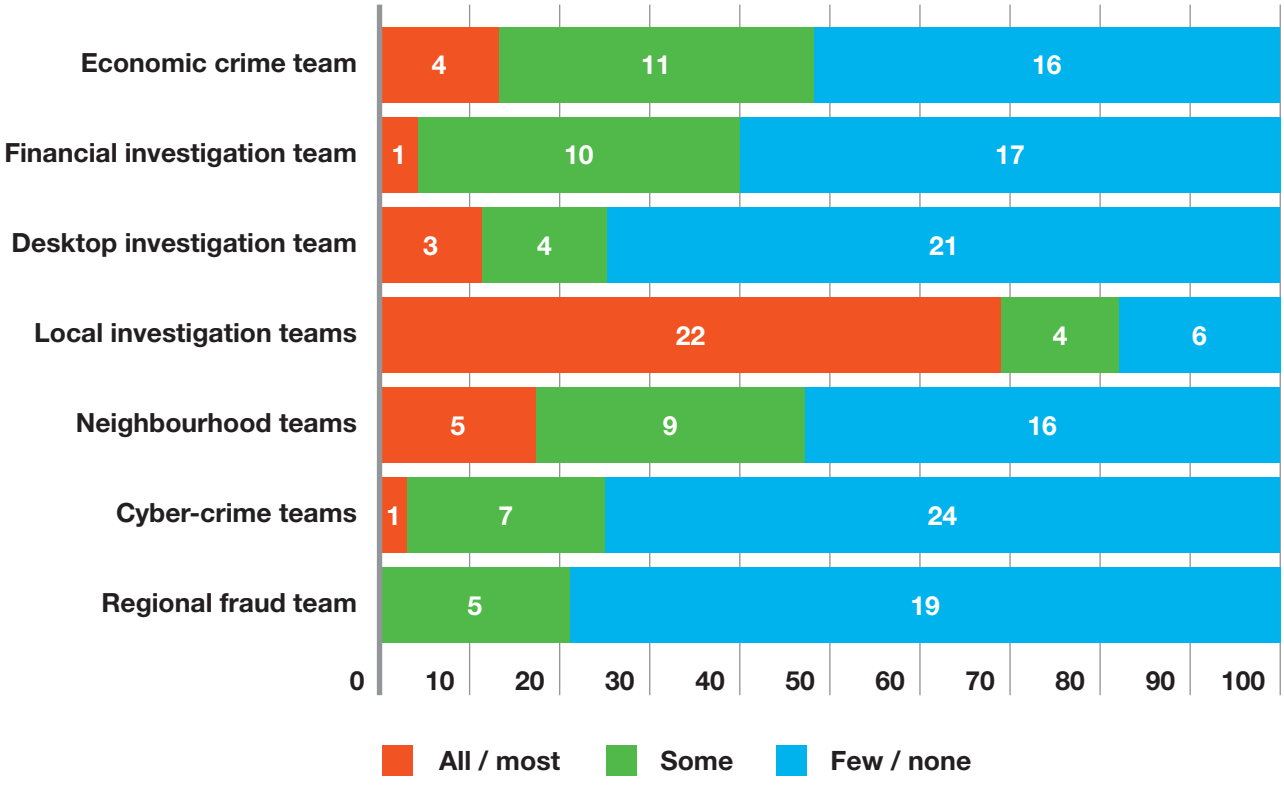
> *'we lose people to banks and any other sector. There's a massive technical skills shortage in cybercrime, investigation and intelligence … anyone with a pinch of knowledge and you are a desirable resource.'*

The generalist police workforce

Given how different fraud is compared to most other types of crime dealt with by local forces (see below) it is surprising that most fraud investigations are handled by generalist local police officers. Economic Crime Teams are relatively small and also cover asset recovery and money laundering and so cannot take on the volume of cases passed down by the National Fraud Intelligence Bureau for investigation.

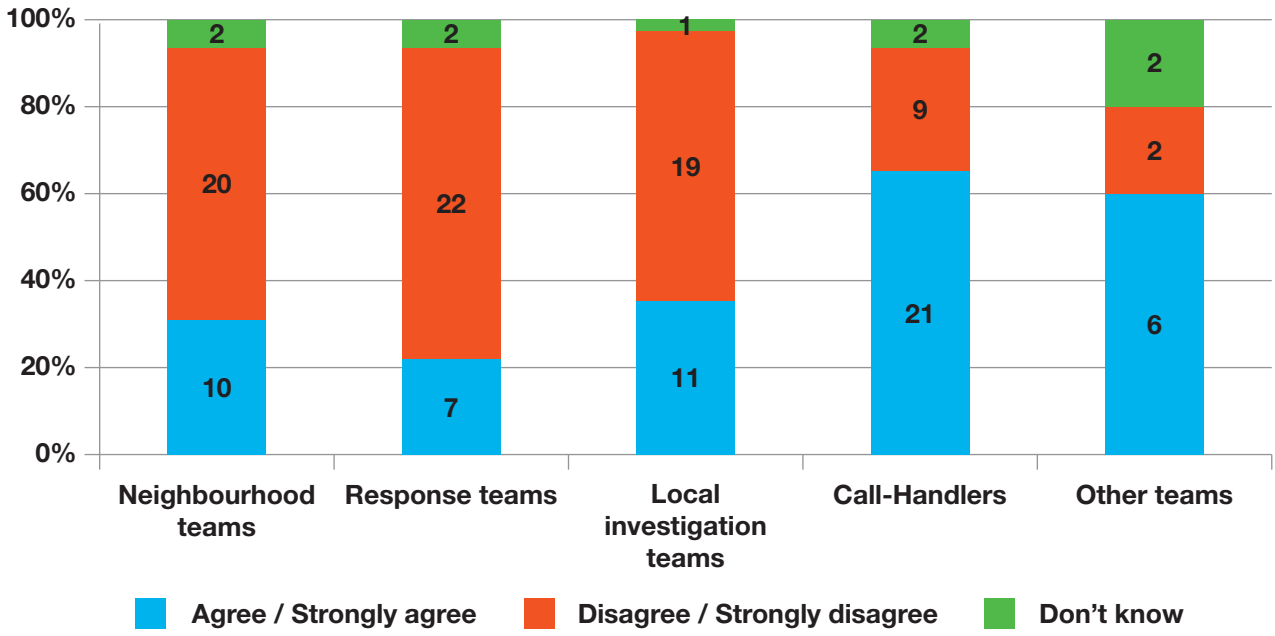
The figure below shows that in 22 out of 32 police forces surveyed generalist local investigation teams deal with all or most fraud investigations [85]. Only a small number reported that Economic Crime Teams (n=4) dealt with all

FIGURE 23: Estimated proportions of fraud investigations conducted by each police team.



[84] Includes outcomes in which an offender is charged / summonsed, cautioned (youths and adults) and community resolutions.
[85] As estimated by the local strategic lead within each police force.

FIGURE 24: Extent to which police force leads agree that teams receive sufficient training.



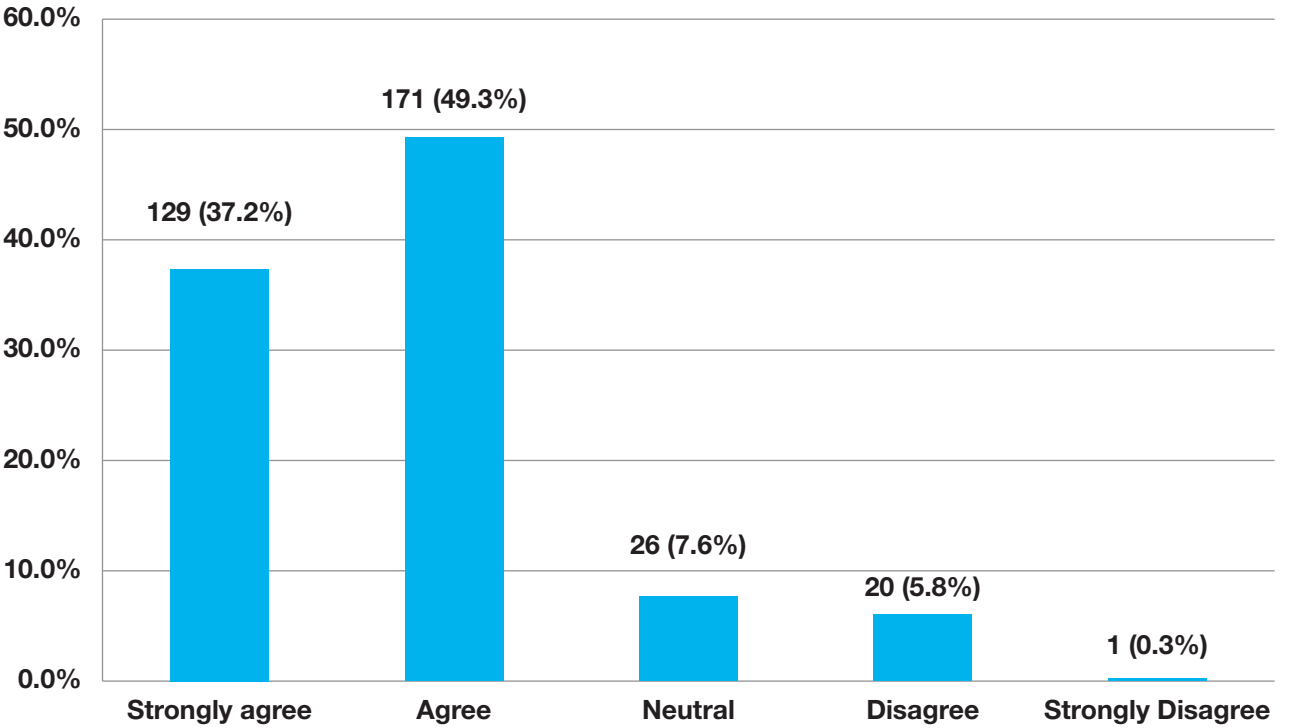
or most fraud investigations, contrasting with other police forces in which neighbourhood teams (n=5) undertook the majority of this work. It is also notable that many other specialist teams had a limited role in investigating fraud, with respondents reporting local cybercrime (75 per cent), financial investigation (61 per cent) or regional teams (79 per cent) conducting few or no fraud investigations.

However, in our survey of strategic leads for fraud, 69 per cent felt that the lack of knowledge in the workforce was one of the most challenging factors in delivering local fraud investigation. As one of the lead officers told us:

> *'There appears to be a general/institutional lack of knowledge and awareness of fraud by frontline officers and staff and their supervisors.'*

A high proportion of the strategic leads in the police believed insufficient training was provided to practitioners in their local investigation (61 per cent), neighbourhood (62.5 per cent) or response teams (71 per cent). This

FIGURE 25: Police workforce attitudes on whether fraud should be dealt with by specialists.



perception was echoed in our workforce survey with the majority (81 per cent) agreeing that fraud policing requires a different set of skills to other crimes, and most agreeing that they needed more training to deal with fraud (78 per cent) and cybercrime (81.5 per cent).

The next Figure (Figure 25) shows that the considerable majority (86 per cent) of respondents to our survey in three police force areas believed fraud should be dealt with by specialists.

This may partly be about skills, but it is also partly about the capacity within the general workforce to take fraud on. In our workforce survey 74 per cent disagreed that they had enough time to deal with a fraud case or victim. A point frequently raised was the intricate and administrative nature of fraud investigation enquiries that demand time and attention they do not have, due to all other demands placed on them as front line practitioners. As one survey respondent told us, the deficiency is less about specialist skills and more a need for a *dedicated* resource with the time and energy that those on the ground feel they do not have:

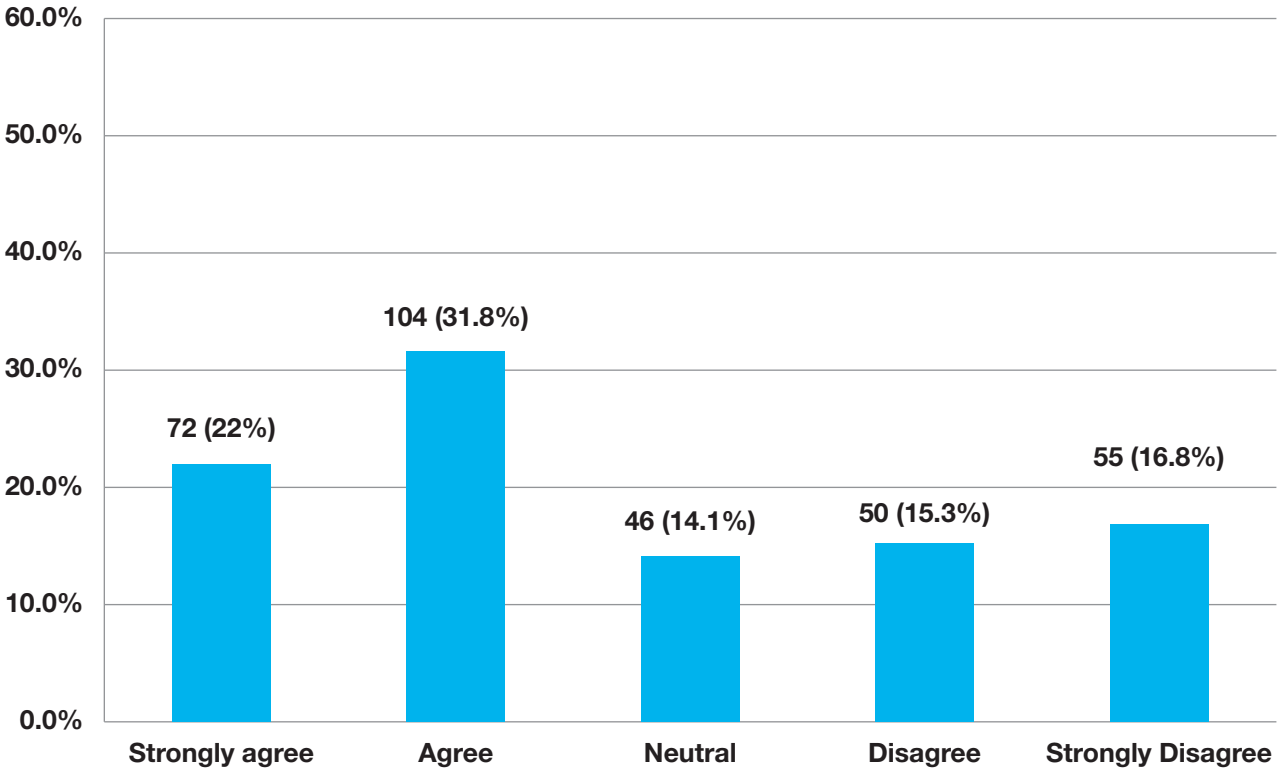
> *'I would be more than happy to deal with more fraud if we were actually given the time to deal with it! The reason it needs to go to a dedicated team is so that it can receive [the required level of time invested].'*

Encouragingly, as Figure 26 below shows, over half (52 per cent) of respondents to our workforce surveys said they would consider specialising in fraud or cybercrime (though many of the comments referred to cybercrime instead of fraud).

There may be cost effective options for expanding fraud investigation teams given that they do not need to be staffed by police officers. Much fraud investigation constitutes desk-top enquiries for which neither boots on the ground, nor a sworn officer status are necessary. The police and NCA have looked to fill the gaps in capability by recruiting civilian volunteers, particularly those with relevant skills for tackling cybercrime [86]. A high proportion of Economic Crime Teams were comprised of civilian staff members. In Avon and Somerset, many fraud investigations are conducted by civilian desktop investigators who deal with a wide range of criminality as a means of 'protecting the front lines', though some felt less valued than officers and received insufficient training to cope with fraud.

> *'Police officers have more powers, but you can give civilians more powers … start with officers and then bring in other staff when established … more cost-effective, they're cheaper... don't need a police officer to do all this stuff, there's no point, they're more expensive.'*

FIGURE 26: Police workforce attitudes on whether they would consider specialising in fraud or cybercrime.



[86] For example, see http://www.nationalcrimeagency.gov.uk/careers/specials [Accessed 30.07.2018].

While not a representative sample, out of 25 fraud case files examined from Avon and Somerset, nine went no further than a civilian investigator and in 15 cases (conducted by a desktop team and/or local police officers) the investigation went no further than preliminary desk-based enquiries such as gathering evidence or statements from victims (by email, phone or by liaising with other police forces) or applying for information from external agencies. Local sworn officers are needed to make arrests and seize evidence but in many cases (especially those perpetrated online or by phone) the investigation never got that far.

From our interviews and two surveys, the following aspects of fraud investigation were highlighted as reasons why it might be better managed by a dedicated specialist workforce:

- The nature of the evidence and the processes required to obtain it is very different to other forms of investigative work local police officers undertake. It includes submissions to banks and other organisations in the private sector and the processing of digital evidence can mean lengthy and complex processes and require investigators to set clear parameters as cases unravel.
- The need to establish relationships with the necessary stakeholders in the public or private sector, which is more easily done if one has regular contact:

  '[The benefit of a central unit is] *also contacts. Keeping regular contact with banks, gumtree, ebay, supermarkets would be so much better.'*
- There is a vast range of changing and complex *modus operandi* in fraud which require decoding, which means generalist officers are regularly faced with the unfamiliar.
- The need to make effective use of legislation.
- The experience required to know when to proceed with an investigation or not.
- There are technical skills required, particularly in digital policing. Our national survey found that while most considered their staff were competent in elements of investigation such as collecting financial evidence (75 per cent) or providing advice and support to fraud victims(79 per cent), many considered that staff in their police force had insufficient skills to investigate cybercrime (59 per cent). These include techniques for digital evidence gathering from online communication or finance where there may be an inability to utilise the data and difficulties in grasping the modus operandi in online offending:

  'It's a very different crime scene, policing has experience with physical crime scenes [in which they are more effective] *… it's a whole different feel to it, not so immediate, people have lost their livelihoods, their life-savings … Need to adapt to a different type of crime scene management … it's a virtual crime scene, not so tangible.'*
- The cross jurisdictional nature of the work, with perpetrators that offend across police force or national borders, or as part of a network or are involved in money laundering.These are the hallmarks of crime that would in other contexts be dealt with as organised crime and would receive a more sophisticated response.
- Overall, there was a problem that because most officers do not deal with fraud cases very often they do not have the opportunity to learn and develop skills.
- Generalist investigators work to a diverse set of priorities and with wide-ranging caseloads and fraud related victimisation (especially that targeting businesses) can be devalued by officers who are directed to prioritise physical harm (for example violence or sexual offences) over financial.

While many practitioners view fraud and related cybercrime investigation as a specialist area it is not recognised as a specialism within the police service, unlike for example financial investigation which has been professionalised and has its own career path. Police officers who gain experience and receive training in fraud are more likely to work in specialist fraud teams but they will have little professional incentive to remain there. The police neither recruit nor promote on the basis of a professional interest in tackling fraud or cybercrime (or indeed any other specialism), but on the basis of generic policing competencies, with a focus on hierarchy over specialism. Comments from our workforce survey indicated that practitioners would be reluctant to enter into a role that has a focus on fraud, and in a number of police forces Economic Crime Teams were staffed by long-serving officers nearing the end of their service or who have already retired and returned as civilian investigators.

'I enjoy the variety of my work and to deal solely with fraud would make me less enthusiastic.'

'It's not the [glamorous] *side of policing,* [appealing to] *officers leading up to retirement, very*

methodical, who like a good spread sheet … investigating from afar.'

In addition to the lack of skills and knowledge, our interviews and surveys picked up evidence of a lack of inclination to pursue fraud cases among the general workforce. Fraud investigations are seen as protracted and considered unlikely to lead to a prosecution. These are key considerations that drive decision-making on what is proportionate or in the public interest, when assessing which investigations to take forward. For this reason, investigation teams complete preliminary assessments and there are often many reasons to rule out pursuing fraud cases on the basis of the degree of loss and how complex the investigation is likely to get. One practitioner stated some police forces will not investigate if the money has been moved outside the UK. One respondent summarised as follows:

'People don't like fraud, police officers don't like investigating fraud, a lot of investigations just go nowhere.'

While some officers sympathise with the victims, fraud is perceived to be occurring in volumes that are unfeasible for the police with limited resource to manage. This in part reflects a lack of reach to intervene against offenders impacting from afar. Nearly half (49 per cent) of the police officers and staff in our survey agreed or strongly agreed that other organisations would be better placed to deal with fraud – these were commonly national-level organisations such as the National Crime Agency (NCA) or other national agency, financial service providers or web companies. This is partly connected with a widespread perception that the only worthwhile approach to fraud is to prevent it.

'Quite simply the police do not have the resources to deal with the level of fraud that we're now seeing. There's no chance of preventing it through a police approach and it does take all sectors sorting themselves out to help prevent it.'

A better use of the workforce: dedicated regional investigation units

We have found that fraud is deemed neither serious enough to attract interest from the NCA or Regional Organised Crime Units nor local enough to gain traction within local forces. It falls between these specialist and local stools. Most fraud investigations end up being carried out by local generalist officers who say they lack the knowledge and skills to carry out this role effectively. While we accept that given the varying size of police forces one size may not fit all, for most of the country we believe that both complex and volume fraud investigation should not be handled by general police investigators but rather housed within regional fraud units with dedicated investigators, many of whom need not be police officers. This reform would improve the efficiency and effectiveness of fraud investigation because:

- Fraud investigation is different from most other types of local crime investigation and requires a set of skills and relationships that generalist officers do not possess.
- Most fraud investigations are desk based and do not require the same kind of physical presence necessitated during other local investigations.
- Dedicated teams of fraud investigators would build up skills, knowledge, networks and overall capability such that they should be able to investigate frauds more quickly and effectively. Even if the number of frauds investigated under this system is fewer than at present we believe that it is better to achieve a smaller number of successful investigations than it is to allocate a larger number most of which are not prioritised or successful.

These fraud teams should not simply duplicate the work of Economic Crime Teams on complex or serious cases (although they probably ought to be co-located), but rather should focus on volume fraud of the kind currently allocated to generalists but with a focus on tackling it more effectively. These regional fraud teams should be accountable to the City of London Police as part of a fraud network, in much the same way as the counter terrorism network functions. Although they should probably be co-located with Regional Organised Crime Units and will obviously work in partnership with them.

Recommendation 27: All fraud investigations should be handled by dedicated investigators, housed mainly in regional fraud investigation units. These would include specialists currently working in Economic Crime Teams leading on large and complex frauds, and volume fraud that is currently allocated to non-specialist officers. Many of these investigators would not need to be police officers and could be recruited via different channels.

6.5 SUMMARY

This chapter has argued that behind the operational weaknesses identified earlier in this report is a bigger problem: policymakers do not prioritise fraud nationally and as a result the law enforcement system we have in place for tackling it is weak.

We have argued that although the public tends not to prioritise fraud, this on its own is not a good reason for

the lack of attention it receives. In aggregate, fraud causes considerable harm to society, even if it is not always visible, and causes significant harm to individuals, particularly vulnerable victims. While we must be realistic about what can be achieved it is clear to us that there ought to be a greater strategic focus on fraud by the government and policing than there has been hitherto.

Fraud is one of the most pervasive crimes in the UK, affecting three million people a year, and yet there is no national strategy for dealing with it. We recommend that the government should produce a national strategy for tackling fraud and that the City of London Police should develop a supplementary national fraud policing strategy and be responsible for overseeing its implementation. The role of local forces should be clarified and they should be accountable for fulfilling a clearer expectation in the Strategic Policing Requirement. This should focus on coordinating local efforts on fraud prevention and supporting vulnerable victims.

Most significantly we do not believe that local policing is best placed to carry out investigations into fraud and recommend that this should be done by dedicated regional fraud investigations units.

CONCLUSION

This report represents a clarion call for greater action to tackle fraud. We have shown that there are major deficiencies in the police response to one of the largest components of crime and one which has a significant impact both on society as a whole and on individual victims.

Fraud enforcement activity will only ever be part of the solution, but it is nonetheless an important part of the response to fraud. Laws need to be enforced if we are to sustain public confidence in the criminal justice system and victims of fraud deserve justice like victims of other crimes. Fraudsters need to know that there is a chance of being caught.

While fraud investigations are intrinsically complex, there are ways in which the enforcement response could be strengthened. Reporting channels need to be improved to encourage reporting and secure better information from victims. The gap between the national bodies responsible for understanding the problem and the local police forces responsible for fraud investigations needs to be reduced. In part this can be dealt with by more standardised systems and protocols for handling cases and assessing threat and harm. However, we argue that there needs to be a more radical move: fraud investigations should be taken off local police forces and handled by a national network of regional investigation units answerable to the City of London Police.

Victims of fraud have some basic expectations of a service, even in the event that they will not get their money back or that the offender is not detected. The response system is currently falls far short of providing this basic level of service to victims. There needs to be a set of national minimum standards for the service fraud victims can expect from policing, covering victims who do not get an investigation, those who do and those who are vulnerable. The aim should be to provide a single seamless service to victims of fraud with the same basic standards wherever they live. There should be a national unit to assess the needs of vulnerable victims and make local referrals.

Prevention is rightly seen as the best way to tackle a volume, cross border crime like fraud, for which the pursuit of offenders can only ever be a small part of the effort. We have identified a number of promising initiatives around the country, including lots of awareness campaigns and work targeted at some vulnerable groups.

However, we also found major gaps in the effort to prevent fraud. Public awareness and education campaigns are fragmented and we lack an evidence base on their impact. Locally, prevention work is poorly led and coordinated. There needs to be a much clearer delineation of roles and responsibilities so that messaging is consistent and the impact of different initiatives adds up to more than the sum of their parts.

Behind these operational weaknesses is a bigger problem: policymakers do not prioritise fraud nationally and as a result the law enforcement system we have in place for tackling it is weak. We need a national strategy to tackle fraud with clear lines of accountability for implementation. The role of local policing in particular needs to be clarified and changed. Police forces and local PCCs should focus on supporting vulnerable victims and coordinating local prevention work, while fraud investigations should be carried out by dedicated regional teams working within an accountable national network.

We do not pretend that if implemented, these recommendations will transform the way in which we deal with fraud. The truth is that fraud is a volume crime affecting society at a time of resource constraint. There are also more pressing issues demanding additional resource. However we think that a greater strategic focus allied to the reforms we have set out could make a difference and improve the service for those UK citizens affected by fraud.

REFERENCES

Age UK (2015) *Only the tip of the iceberg: Fraud against older people: Evidence review.* London: Age UK.

Association of Chief Police Officers (2005) *National Call Handling Standards*. London: Home Office.

Betts, M. (2017) *Investigation of Fraud and Economic Crime*. Oxford: Oxford University Press.

Bjorgo, T. (2015) *Preventing Crime: A Holistic Approach*. Basingstoke: Palgrave.

Blakeborough, L. and Correia, S. (2018) *The scale and nature of fraud: A review of the evidence*. London: Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf [Accessed 29 September 2018].

Blum-West, S., and Carter, T. J. (1983) *Bringing white-collar crime back in: an examination of crimes and torts*. Social Problems, 30(5), 545-554.

Bossler A. M., and Holt T. J. (2012) 'Patrol officers' perceived role in responding to cybercrime'. *Policing: An international Journal of Police Strategies & Management*, 35 (1), pp. 165-181.

Brown, R., Evans, E., Webb, S., Holdaway, S., Berry, G., Chenery, S., Gresty, B. and Jones, M. (2012) *The Contribution of Financial Investigation to Tackling Organised Crime: A Qualitative Study*. London: Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116518/horr65.pdf [Accessed 2 September 2018].

Bullock K., Clarke R. V., and Tilley, N. (2010) *Situational Prevention of Organised Crimes*. Cullompton: Willan Publishing.

Button, M., Lewis, C., and Tapley, J. (2009a) *Support for the victims of fraud: An assessment of the current infrastructure in England and Wales*. London: NFA.

Button, M., Lewis, C., and Tapley, J. (2009b) *A better deal for fraud victims: Research into victims' needs and experiences*. London: NFA.

Button, M., Lewis, C., Shepherd, D., Brooks, G. and Wakefield, A. (2012) *Fraud and Punishment: Enhancing Deterrence Through More Effective Sanctions*. Portsmouth: University of Portsmouth.

Button, M., Lewis, C., and Tapley, J. (2014) 'Not a victimless crime: The impact of fraud on individual victims and their families'. *Security Journal*, 27 (1), pp. 36–54.

Button, M., Nicholls, C., Kerr, J., and Owen, R. (2014a) 'Online frauds: Learning from victims why they fall for these scams'. *Australian & New Zealand Journal of Criminology*, 47 (3), pp. 391-408.

Button, M., Blackbourn, D., and Tunley, M. (2014b) 'The Not So Thin Blue Line After All?' Investigative Resources Dedicated to Fighting Fraud/Economic Crime in the United Kingdom'. *Policing: A Journal of Policy and Practice*, 9 (2), pp.129-142.

Button, M., Blackbourn, D. and Shepherd, D. (2016) *The Fraud 'Justice Systems': A Scoping Study on the Civil, Regulatory and Private Paths to 'Justice' for Fraudsters*. University of Portsmouth.

Button, M. and Cross, C. (2017) Cyber Frauds, *Scams and their Victims*. London: Routledge.

Button, M., Gee, J., and Mothershaw, N. (2017) *Annual Fraud Indicator 2017: Identifying the Cost of Fraud to the UK Economy*. Crowe Clark Whitehill, University of Portsmouth and Experian.

City of London Police (2017) *National Policing Lead For Economic Crime: Annual Report 2016-17*. Available at: https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Pages/Annual-Review.aspx [Accessed 15 August 2018].

Clarke, R. V. (1995) Situational crime prevention. *Crime and Justice*, 19, 91-150.

Clarke, R.V. (ed.) (1997) *Situational Crime Prevention: Successful Case Studies* (2nd ed.) New York: Harrow and Heston.

Clarke, R. V., and Weisburd, D. (1994) 'Diffusion of crime control benefits: Observations on the reverse of displacement'. *Crime Prevention Studies*, 2, pp.165-184.

College of Policing (2015) *College of Policing analysis: Estimating demand on the police service*. College of Policing. Available at: http://www.college.police.uk/About/Pages/Demand-Analysis-Report.aspx [Accessed 15 August 2018].

Cornish, D. B., and Clarke, R. V. (1987) 'Understanding crime displacement: An application of rational choice theory'. *Criminology*, 25 (4), pp. 933-948.

Cornish, D. B., and Clarke, R. V. (2002) 'Analyzing organized crime' *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. London: Routledge.

Cornish, D. B., and Clarke, R. V. (2008) 'The rational choice perspective'. *Environmental Criminology and Crime Analysis*, 21, 21-47.

Couture, X., and Pardoe, A. (2017) *Changing the story on scams: Protecting consumers and increasing reporting*. London: Citizens Advice.

Crocker, R., Webb, S., Garner, S., Skidmore, M., Gill, M., and Graham, J. (2017) *The impact of Organised Crime in Local Communities*. London: The Police Foundation.

Cross, C., and Blackshaw, D. (2014) Improving the Police Response to Online Fraud. *Policing: A Journal of Policy and Practice*, 9(2), pp. 119-128.

Cross, C. (2015) 'No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21 (1), pp. 187-204.

Cross, C., and Kelly, M. (2016a) 'The problem of "white noise": examining current prevention approaches to online fraud'. *Journal of Financial Crime* 23 (4), pp. 806-818.

Cross, C., Richards, C., and Smith, R. (2016b) 'The reporting experiences and support needs of victims of online fraud'. *Trends and Issues in Crime and Criminal Justice*, 518, pp. 1-14.

Dalley, G., Gilhooly, M., Gilhooly, K., Levi, M., and Harries, P. (2017) 'Researching the financial abuse of individuals lacking mental capacity'. *The Journal of Adult Protection*, 19 (6), pp. 394-405.

Dedicated Card and Payment Crime Unit (DCPCU) (2015) *Project Skynet*, unpublished.

Deevy, M., Lucich, S. and Beals, M. (2012) *Scams, schemes and swindles: A review of consumer financial fraud research*. Stanford: Stanford University.

Doig, A., and Levi, M. 2013 'A case of arrested development? Delivering the UK National Fraud Strategy within competing policing policy priorities'. *Public Money and Management*, 33 (2), pp. 145-152.

Ekblom, P. (2011) *Crime Prevention, Security and Community Safety Using the 5Is Framework*. Basingstoke: Palgrave.

Farrell G., Bowers K. J., and Johnson S. D. (2013) 'Cost-benefit analysis for crime science: Making cost-benefit analysis useful through a portfolio of outcomes. In': Tilley and Smith (eds.) *Crime Science: New Approaches to Preventing and Detecting Crime*. Willan Press.

Federation of Small Businesses (FSB) (2016a) *Cyber Resilience: How to Protect Small Firms in the Digital Economy*. London: FSB.

Federation of Small Businesses (FSB) (2016b) Business Crime – FSB Survey, unpublished.

Financial Ombudsman Service (2015) *Calling Time on Telephone Fraud: a Review of Complaints about "Vishing" Scams*. Financial Ombudsman Service.

Fraud Advisory Panel (2005) *The Fraud Advisory Panel Seventh Annual Review 2004-2005: The Human Cost of Fraud*. London: Fraud Advisory Panel.

Fraud Advisory Panel (2012) *Obtaining redress and improving outcomes for the victims of fraud: Research into the professional advice given to victims of fraud trying to recover their money*. London: Fraud Advisory Panel.

Fraud Advisory Panel (2016) *Ten years on from the 2006 'The Fraud Review'*. London: Fraud Advisory Panel. Available at: https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf.

Gannon, R., and Doig, A. (2010) 'Ducking the answer? Fraud strategies and police resources'. *Policing & Society*, 20(1), pp. 39-60.

Garner, S., Crocker, R., Skidmore, M., Webb, S., Graham, J., and Gill, M. (2016) *Reducing the Impact of Serious Organised Crime in Local Communities - Briefing 1: Organised fraud in local communities*. London: The Police Foundation.

Gill, M. (2011) Learning From Offenders' Accounts of their Offending. *Prison Service Journal*, 194, pp. 27-32.

Gill, M., and Howell, C. (2017) *Police Views on Private Security*. Tunbridge Wells: Perpetuity Research.

Gill, M. (2018) 'A Nick Tilley perspective on preventing opportunistic insurance fraud'. Farrell, G. and Sidebottom (eds) A. *Realist Evaluation for Crime Science: Essays in Honour of Nick Tilley*. London: Routledge.

Greenfield, V. A., and Paoli, L. (2013) 'A framework to assess the harms of crimes'. *British Journal of Criminology*, 53(5), pp. 864-885.

Hales, G. and Higgins, A. (2016) *Prioritisation in a changing world: seven challenges for policing*. London: The Police Foundation.

Haynes, A. (2012) 'Market abuse, fraud and misleading communications' *Journal of Financial Crime*, 19 (3), pp. 234-254.

Higgins, A. (2018) *The future of neighbourhood policing*. London: The Police Foundation.

Hinduja, S. and Kooi, B. (2013) Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal October*, Volume 26, Issue 4, pp 383–402.

HM Government (2006) *Fraud Review: Final Report*. Accessible at:http://webarchive.nationalarchives.gov.uk/20070222120000/http://www.lslo.gov.uk/pdf/FraudReview.pdf [Accessed 5 August 2018].

HM Government (2013) *Serious and Organised Crime Strategy*. London: The Stationery Office.

HM Government (2016) *National Cyber Security Strategy 2016-2021*. London: The Stationery Office.

HMIC (2015) *Real lives, real crimes: A study of digital crime and policing*. London: HMIC.

Holt, T. (2013) Exploring the social organisation and structure of stolen data markets'. *Global Crime*, 14:2-3, pp. 155-174.

Home Office (2015) *The Strategic Policing Requirement*. London: Home Office.

Home Office (2016a). *Modern Crime Prevention Strategy*. London: Home Office.

Home Office (2016b) *Serious and Organised Crime Protection: Public Interventions Model*. London: Home Office. Available at: https://www.gov.uk/government/publications/vulnerability-to-financial-and-cyber-crime-research-on-the-uk-population [Accessed 15 August 2017].

Home Office (2018a) *Home Office Counting Rules for Recorded Crime: Fraud*. Available at: https://www.gov.uk/government/publications/counting-rules-for-recorded-crime [Accessed 3 October 2018].

Home Office (2018b) *Crime outcomes in England and Wales: year ending March 2018*. Available at: https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2017-to-2018 [Accessed 10 September 2018].

Home Office (2018c) *Crime against businesses: findings from the 2017 Commercial Victimisation Survey*. Available at: https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2017-commercial-victimisation-survey [Accessed 5 July 2018].

Hopkins, M. and Gill, M. (2017) Business, crime and crime prevention: emerging debates and future challenges. In Tilley, N. and Sidebottom, A. (eds) *Handbook of Crime Prevention and Community Safety*, 2nd edition. London: Routledge.

Howell, C., Horton, T., and Gill, M. (2013) *Financial Investigation: Identifying the True Value*. Tunbridge Wells: Perpetuity Research.

Hutchings, Al, Clayton, R. and Anderson, R. (2016) *Taking Down Websites to Prevent Crime*. eCrime Researchers Summit, eCrime, 2016-June 102-111.

Innes, H. and Innes, M. (2013) Personal, *Situational and Incidental Vulnerabilities to ASB Harm: a follow up study*. Cardiff: Cardiff University.

Ipsos MORI (2017) *Public Perceptions of Policing in England and Wales 2017: Report for Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services*. London: Ipsos MORI.

Kurpjuhn, T. (2015). 'The SME security challenge'. *Computer Fraud & Security*, 3, pp.5-7.

Levi, M. (2008) Organized fraud and organizing frauds: Unpacking research on networks and organization, *Criminology & Criminal Justice*, 8(4), pp. 389-419.

Levi, M. (2008a) 'Policing fraud and organised crime'. In: Newburn, T. (ed) *Handbook of Policing*. Cullompton: Willan Publishing.

Levi, M. (2010). Public and private policing of financial crimes: the struggle for co-ordination, *Journal of Criminal Justice and Security*, 12(4), pp. 343-354.

Levi, M. and Maguire, M. (2012) Something old, something new; something not entirely blue: Uneven and shifting modes of crime control. Newburn, T., and Peay, J., *Policing: Politics, Culture and Control*. Oxford: Hart Publishing.

Levi, M., and Williams, M. L. (2013) 'Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space'. *Information Management & Computer Security*, 21(5), pp. 420-443.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. (2015) *The Implications of Economic Cybercrime for Policing*. London: City of London Corporation.

Levi, M. and Schuchter, A. (2015) 'Beyond the fraud triangle: Swiss and Austrian elite fraudsters'. *Accounting Forum* 39(3), pp. 176-187.

Lonsdale, J., Schweppenstedde, D., Strang, L., Stepanek, M., and Stewart, K. (2016) *National Trading Standards – Scams Team Review*. Cambridge: RAND.

Lord, N., Spencer, J. Albanese, J., and Elizondo, C.F (2017) 'In pursuit of food system integrity: the situational prevention of food fraud enterprise'. *European Journal on Criminal Policy and Research*, 23 (4), pp. 483–50.

Loveday, B. (2017) Still Plodding Along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science & Management*, 19(2), pp. 101-109.

Lusthaus, J. and Varese, F. (2017) Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, pax042.

May, T., and Bhardwa, B. (2018) *Organised Crime Groups involved in Fraud*. Palgrave: London.

McGuire and Dowling (2013) *Cyber crime: A review of the evidence. Research Report 75. Summary of key findings and implications*. London: Home Office.

Mills, H., Skodbo, S., and Blyth, P. (2013) *Understanding organised crime: estimating the scale and the social and economic costs*. London: Home Office.

Ministry of Justice (2015) *Code of Practice for Victims of Crime*. Available at: https://www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime [Accessed 15 January 2018].

National Audit Office (NAO) (2016) *Protecting consumers from scams, unfair trading and unsafe goods*. London: National Audit Office.

National Audit Office (2017) *Online Fraud*. London: National Audit Office.

National Crime Agency (2016) *NCA Strategic Cyber Industry Group: Cyber Crime Assessment 2016*. London: NCA.

National Crime Agency (2018) *National Strategic Assessment of serious and organised crime 2018*. London: NCA.

National Fraud Authority (2011) *A quantitative segmentation of the UK population: Helping to determine how, why and when citizens become victims of fraud*. London: National Fraud Authority.

National Fraud Authority (2013). *Annual Fraud Indicator*. London: National Fraud Authority.

National Fraud Strategic Authority (2011) *The National Fraud Strategy: A new approach to combating fraud*. London: National Fraud Strategic Authority.

Office for National Statistics (2016a) *Overview of fraud statistics: year ending March 2016*. London: ONS. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016 [Accessed 18 October 2018].

Office for National Statistics (2016b) *Research outputs: developing a crime severity score for England and Wales using data on crimes recorded by the police*. London: ONS.

Office for National Statistics (2018a) *Crime in England and Wales: year ending March 2018*. London: ONS. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018 [Accessed 5 October 2018].

Office for National Statistics (2018b) *Overview of fraud and computer misuse statistics for England and Wales*. London: ONS.

Pascoe, T., Owen, K., Keats, G., and Gill, M. (2006) *Identity Fraud: What about the Victim?* Leicester: Perpetuity Research.

Phillips, C. (2017) *From 'Rogue Traders' to Organized Crime Groups: Doorstep Fraud of Older Adults*. British Journal of Criminology, 2017(57), 608-626.

Pritchard, S. (2010) *Navigating the black hole of small business security*. *Infosecurity*, 7(5), pp.18-21.

Renaud, K. (2016) How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8), 10-18.

Roberts, J. V., and Hastings, R. (2012) Public opinion and crime prevention: A review of international trends, in Welsh, B. C., & Farrington, D. P. (2012). *The Oxford Handbook of Crime Prevention*. Oxford University Press.

Sandywell, B. (2009) On the globalisation of crime: the Internet and new criminality. in Jewkes, Y. and Yar, M. (eds) *Handbook of Internet Crime*. Cullompton: Willan.

Scholes, A. (2018) *The scale and drivers of attrition in reported fraud and cyber crime: Research Report 97*. London: Home Office.

Sherman, L. W., Farrington, D. P., and Welsh, B. C. and MacKenzie, D. L., (eds.). (2002) *Evidence-based Crime Prevention*. New York: Routledge.

Sherman, L. W. (2013) Targeting, testing and tracking police services: The rise of evidence-based policing. In M. Tonry, ed., Crime and Justice in America, 1975-2025. *Crime and Justice 42*. Chicago: University of Chicago Press.

Sutherland, E. H., Geis, G., and Goff, C. (1983) *White collar crime: The uncut version (Vol. 58)*. New Haven, CT: Yale University Press.

Tilley N, Farrell G (eds) (2012) *The reasoning criminologist. Essays in honour of Ronald V. Clarke*. Routledge, London.

Tunley, M., Button, M., Shepherd, D. and Blackbourn, D. (2018) Preventing occupational corruption: utilising situational crime prevention techniques and theory to enhance organisational resilience. *Security Journal*, February, Volume 31, Issue 1, pp 21–52.

UNODC (2010). *Handbook on the crime prevention guidelines: Making them work*. Criminal Justice Handbook Series. New York: United Nations.

Von Lampe K (2011) The application of the framework of situational crime prevention to 'organized crime'. *Criminology, Crime and Justice* 11(2):145–163.

Walby, K. and Lippert, R. (2014) (eds) *Corporate Security in the 21st Century*. Basingstoke: Palgrave.

Wall, D. (2007) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice & Research: An International Journal*, 8(2):183 205.

Wedlock, E. and Tapley, J. (2016) *What works in supporting victims of crime: A rapid evidence assessment*. London: Victims Commissioner.

Weisburd, D., and Eck, J. E. (2004) What can police do to reduce crime, disorder, and fear? *The Annals of the American Academy of Political and Social Science*, 593(1), 42-65.

Welsh, B. (2018) *Costs and benefits of preventing crime*. Routledge.

Whitty, M. and Buchanan, T. (2015) The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice*, Volume:16, Issue: 2, page(s): 176-194.

Whitty, M. (2018) Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behaviour and Social Network*. 2018 Feb 1; 21(2): 105–109.

Williams, M. L., and Levi, M. (2017). Cybercrime prevention in Tilley, N., and Sidebottom, A. (Eds.). (2017). *Handbook of crime prevention and community safety*. Taylor & Francis, pp 454 to 469.

APPENDICES

APPENDIX A: METHODOLOGY

Literature review

The review was conducted with a main focus on research in the UK, incorporating research from overseas where especially pertinent. Sources included peer-reviewed academic articles, reports, and anything else deemed relevant. The primary focus was on:

- Understanding fraud – the scale and nature of fraud, the links with cyber crime, and the relationship between these and police structures and priorities
- The scale of victimisation and underreporting, victim characteristics, the demographics of those victimised, vulnerability, the impact and harm of fraud, and what victims want
- The police and criminal justice – response structures at the local level, the effectiveness of enforcement, the role of specialist enforcement
- The role and priorities in fraud and cyber crime prevention

Practitioner interviews

The researchers conducted in-depth face-to-face and telephone interviews with key stakeholders working in local police forces, national organisations and victim services organisations. A purposive sampling strategy was employed, based on continuous review of interview data against the aims of the project and the judgement of the research team.

The interviews were conducted by four researchers who shared and reviewed the evidence provided in order to identify any emerging themes or gaps in knowledge. 107 interviews were conducted in total and Table A1 and A2 below, provide a broad outline of the organisations and the roles of those interviewed. Interviews lasted between one and two hours and were semi-structured, using an interview schedule that built upon the findings of the evidence review and was piloted with stakeholders from relevant agencies. Detailed notes were taken throughout each interview, including verbatim quotes.

Preliminary interviews were carried out with frontline staff working in enforcement and victim care roles in Avon and Somerset, Kent, and Essex police forces in order to gain an in-depth understanding of operational structures and front line issues when managing fraud and working with fraud victims. Subsequent interviews with regional and national stakeholders and practitioners in other police force areas provided additional and important insights that set a broader context for the work.

TABLE A1: A breakdown of practitioners interview by organisation/sector.

Organisation	No. Interviews *
Kent and Essex Police	20
Avon and Somerset Police	19
City of London Police (incl. Action Fraud and NFIB)	18
Other Police Force	6
Specialist Regional / National Enforcement	4
Trading Standards	5
Other Public Sector	2
Third Sector	22
Other National Stakeholder – Public Sector	11
Total	**107**

* A number of interviews had more than one practitioner attend and the total number of practitioners was 117.

Practitioners interviewed

Police officers/staff with a range of roles in Avon and Somerset, Kent and Essex and other police force areas were interviewed including those in Economic Crime Teams (n=16), generalist investigators (n=6), neighbourhood or police response teams (n=7), contact centre and crime assessment teams (n=7), victim services (n=5) and strategic economic crime leads (n=4).

From the City of London Police nine staff members from the National Fraud Intelligence Bureau (NFIB) and five from Action Fraud were interviewed. Other interviewees were individuals in strategic or specialist roles including an investigator from the Dedicated Card and Payment Crime Unit.

Interviews were completed with range of policy staff (including lobbyists) and practitioners outside of local police forces including stakeholders in government, the National Police Chiefs' Council, regional and national enforcement agencies, Trading Standards and third sector advocacy and support services. Interviewees ranged from national policy officials to local-level practitioners. A breakdown is provided in Table A2 below.

National police force survey

The strategic leads in all police forces were surveyed to provide a national perspective on the diverse response structures, processes and priorities across local police force areas. The questions in the survey were drawn from emerging findings from interviews and consultation with police stakeholders.

The survey was disseminated to all 43 police forces in England and Wales. The survey was disseminated by HMICFRS alongside other procedural data-requests sent to police forces prior to an inspection programme. However, the survey was identified to forces as an independent piece of work and they were informed that their responses would not be used for inspection purposes and all data would be anonymised. In order to obtain an authoritative perspective of the approach in each police force it was requested that the strategic lead for fraud take the lead in completing the survey (with input from other personnel where necessary). The extent to which each police force followed this instruction cannot be certain.

A total of 32 surveys were completed and returned. It should be noted that a number of the largest metropolitan forces did not return a survey which may impact on the representativeness of the findings. The ranking of respondents ranged from detective superintendent (n=5) to detective sergeant (n=3). 'Other' categories (n=3) included the manager of a relevant unit (possibly civilian personnel). Table 1 shows that out of the 32 surveys returned, 80 per cent were completed by an officer of detective inspector rank or above.

TABLE A2: Organisations consulted outside of local police forces.

Organisation	Interviewees role(s)
Age UK	Policy / Practitioner
Cifas	Policy / Analysts
Citizens Advice	Policy
Federation of Small Businesses	Policy
Fraud Advisory Panel	Policy
HM Inspectorate of Constabulary	Inspectors
Home Office	Policy / Analysts
National Business Crime Centre (hosted by the Metropolitan Police)	Policy
National Crime Agency	Policy / Practitioners
National Cyber Security Centre	Policy
National Police Chief's Council	Policy
Association of Police and Crime Commissioners	Policy
Regional Organised Crime Units	Practitioners
National and Local Trading Standards	Policy / Practitioners
Think Jessica	Policy
Turning Tides	Practitioner
Victim Support	Policy / Practitioners

TABLE A3: The rank and unit for each survey respondent.

	Fraud	Economic Crime	Other Specialist Functions	General Investigations	Other / Unspecified	Total
Detective Superintendents	3	0	1	1	0	**5 (16%)**
Detective Chief Inspectors	0	3	2	0	0	**5 (16%)**
Detective Inspectors	3	8	1	1	2	**15 (48%)**
Detective Sergeants	2	1	0	0	0	**3 (10%)**
Other / Unspecified	0	2	0	0	1	**3 (10%)**
TOTAL	**8 (26%)**	**14 (45%)**	**4 (13%)**	**2 (6%)**	**3 (10%)**	**31**

* No information on rank or department was provided in one police force.

Only a quarter (26 per cent) of respondents described a team role with an explicit focus on fraud (for example, 'fraud investigations' or 'fraud and cybercrime investigations). Most prevalent were respondents from Economic crime teams (45 per cent) which were in some cases responsible for cybercrime as well.

Police workforce survey

In partnership with Avon and Somerset, Kent and Essex a survey of attitudes was disseminated to all members of staff in the three police forces. We received a much higher response rate in Essex and Kent than in Avon and Somerset; total numbers received were 211, 95 and 23 respectively, with the remainder not specifying which police force they were from. This most likely reflects the divergent approaches to disseminating the survey (in the former it was sent by email to all staff whereas in the latter it was attached to an internal circular email). In this regard, the answers are less representative of the Avon and Somerset workforce. The sample includes those in the workforce who voluntarily responded and therefore may not represent the full range of attitudes in the police forces. Also, it was a local survey therefore is not representative of attitudes in all other police forces.

Table A1 outlines the self-reported roles of survey respondents. Over a third (35 per cent) worked in investigation (a small number specialist fraud teams) and a quarter (26 per cent) in a neighbourhood team. A quarter (26 per cent) of respondents did not specify their role in the police force. Out of 340 respondents who provided their police rank, 58 per cent were constables, 20 per cent sergeants and 13 per cent were civilian members of staff. Officers of other ranks and roles were present in smaller numbers, including Police Community Support Officers (two per cent) and those ranked inspector or above (one per cent). The remaining respondents described themselves as 'other' or reported a preference not to answer.

TABLE A4: The self-reported roles of respondents in the workforce survey.

Role	No.
Investigation	125 (31%)
Specialist Fraud and Financial Investigator	16 (4%)
Neighbourhood	104 (26%)
Control Room / Incident Assessment	8 (2%)
Other Police Staff	23 (6%)
Other	25 (6%)
No Response *	104 (26%)
TOTAL	**405**

* Comprised of respondents who left the field blank or reported a preference not to answer.

Trading Standards Offices Survey

With the support of the National Trading Standards Scams team the researchers were able to disseminate an information request by email to *all* Trading Standards

TABLE A5: The criterion applied during the selection of investigations for case file analysis.

Criterion:	Description:
Value of financial loss	Cases in top and bottom 10 per cent in value lost
Number of victims	Crimes that impact on two or more victims
Known offender	Cases with a local identified suspect
Cyber-crime	Fraud cases that were cyber-enabled
Victim	A range of victim types – in particular, businesses and victims recorded as vulnerable
Response	Investigations that reflect the different teams involved in fraud investigation – in particular desktop and local CID
Outcome	Crimes with a range of recorded outcomes, including positive outcome

offices in the UK. The request was for qualitative input on the following elements of the response:

- How they deliver and structure interventions for potential victims flagged by the national scams team.
- Any strategic or tactical partnership arrangements they had in place with others such as the police, voluntary or third sector.
- Any local initiatives developed for tackling any aspect of fraud impacting in your area.
- Specific challenges in tackling fraud in their local area.

We received replies from 21 Trading Standards offices, some of which provided additional strategic assessments or policy documents.

Investigation case file analysis

Twenty-five investigations were selected from a two year sample of local crime data in Avon and Somerset. A purposive sampling strategy was employed to capture as far as possible, the diversity of modus operandi, victims and harm, case allocation and outcomes. The criterion applied during the process of selection is described in Table A5. In each case, both the structured data and the detailed case notes for each investigation were compiled into an anonymised data extract for analysis. The majority of this data were qualitative and need to be structured into themes to reflect the various stages of the investigation and different types of fraud, victim(s) and impact.

This methodology was only possible in Avon and Somerset due to limitations in data access elsewhere. Therefore this sample is not necessarily reflective of the processes in other police forces, many of which operate to different structures and priorities.

APPENDIX B: FRAUD CATEGORISATION

TABLE B1: An index for Home Office fraud offence codes and categories adopted in our analysis (see Table 2, p13 and Figure 2, p17).

Fraud Categorisation	NFIB offence categories
Products or services • Advance fee payments • Financial investments • Non-investment fraud	• "419" Advance fee fraud • Lottery scams • Counterfeit cashiers cheques • Dating scam • Fraud recovery • Inheritance fraud • Rental fraud • Other advance fee frauds • Lender loan fraud • Share sales or boiler room fraud • Pyramid or ponzi scheme • Prime bank guarantees • Time shares and holiday club fraud • Other financial investment • Consumer phone fraud • Computer software service fraud • Ticket fraud • Other consumer (non-investment) fraud
Commercial environment • Online shopping and auction • Retail fraud • Door to door sales and bogus tradesmen • Business trading fraud	• Online shopping and auction • Retail fraud • Door to door sales and bogus tradesmen • Business trading fraud
Industry or sector • Banking and credit industry • Insurance fraud • Telecom industry fraud • Pension fraud • Charity fraud • Public sector fraud	• Cheque, plastic card and online bank accounts (not PSP) • Application Fraud (excluding mortgages) • Mortgage related fraud • Mandate fraud [86] • Dishonestly retaining a wrongful credit • Insurance related fraud • Insurance broker fraud • Telecom industry fraud (misuse of contracts) • Pension fraud by pensioners (or their estate) • Pension fraud committed on pensioners • Pension liberation fraud • Charity fraud • Fraudulent applications for grants from charities or lottery fund organisations • Passport application fraud • Department of works and pensions (DWP) fraud • Fraudulent applications for grants from government organisations • HM Revenue and Customs fraud (HMRC) • DVLA driver licence application fraud
Use of position or occupation • Corporate fraud • False accounting • Bankruptcy and insolvency • Other regulatory fraud • Fraud by failing to disclose information • Abuse of position of trust	• Corporate employee fraud • Corporate procurement fraud • False accounting • Bankruptcy and insolvency • Other regulatory fraud • Fraud by failing to disclose information • Abuse of position of trust

* This table does not include the 'Other' category of fraud.

[86] While mandate fraud does not target specific sectors offenders commonly make use of online bank account transfers to carry out the offence so they were included in this category.

APPENDIX C: DATA TABLES

Recorded fraud patterns analysis

Published data sources used in Figure 1 (p17):

- Office for National Statistics (2018) Crime in England & Wales, year ending March 2018
- Office for National Statistics (2017) Crime in England & Wales, year ending March 2017 – Bulletin tables
- Office for National Statistics (2016) Crime in England & Wales, year ending March 2016 – Bulletin tables
- Office for National Statistics (2014) Crime in England & Wales, year ending March 2014 – Bulletin tables
- 1999/99 to 2010/11 – Home Office (2011) Crime in England and Wales 2010/11: Findings from the British Crime Survey and police recorded crime (2nd Edition) – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116417/hosb1011.pdf

TABLE C1: Volumes of recorded fraud and other acquisitive crimes from 1998 to 2018.

Year	Total No. fraud and forgery offences	Fraud industry figures	Total No. burglary offences	Total No. offences against vehicles	Total No. other theft offences
2017/18	277,561	361,321	437,537	457,036	1,115,124
2016/17	264,060	385,710	411,536	407,057	1,058,165
2015/16	220,691	398,514	401,001	366,248	990,735
2014/15*	230,367	362,744	411,434	351,421	992,268
2013/14	211,228	310,690	443,184	372,307	1,029,752
2012/13	179,891	330,512	459,795	387,360	1,053,793
2011/12	119,426	356,977	501,048	417,442	1,156,289
2010/11**	145,841		522,640	449,681	1,078,727
2009/10	152,241		540,660	494,894	1,037,325
2008/09	163,159		581,584	591,853	1,080,003
2007/08***	155,439		583,710	656,453	1,121,186
2006/07	199,652		622,012	765,015	1,180,802
2005/06	232,774		645,068	792,821	1,226,192
2004/05	280,062		680,358	820,096	1,247,632
2003/04	319,647		820,013	985,006	1,327,884
2002/03	331,098		890,099	1,074,659	1,336,924
2001/02	314,859		878,509	1,064,031	1,202,933
2000/01	319,324		836,027	1,031,143	1,114,229
1999/2000	334,773		906,468	1,100,439	1,123,181
1998/99	279,503		953,184	1,125,737	1,065,702

* 'Making off without payment' offences were previously classified as fraud but from this point onwards, were reclassified as an 'other theft offence'.

** Action Fraud launched and beginning to take over fraud reporting in some police forces – national roll-out was 2013.

*** The first year in which recording was changed by the introduction of the Fraud Act (2006)

Cyber-enabled fraud

TABLE C2: The proportion of fraud categories with a cyber indicator (see Table 3, p22).

Fraud category	At least one cyber indicator	First contact online	Payment taken or sent from account	Total in sample
Online Shopping and Auctions	13,888 (100%)*	11,379 (82%)	10,409 (75%)	13,888
Other Fraud (Not covered elsewhere)	4,580 (62%)	2,931 (40%)	3,164 (43%)	7,365
Other Advance Fee Frauds	2,912 (46%)	1,837 (29%)	2,086 (33%)	6,277
Cheque, Plastic Card and Online Bank Accounts (not PSP)	2,152 (54%)	767 (19%)	1,697 (43%)	3,955
Mandate Fraud	3,550 (94%)	2,843 (75%)	3,011 (80%)	3,774
Retail Fraud	240 (8%)	172 (6%)	164 (5%)	3,127
Computer Software Service Fraud	3,097 (100%)*	190 (6%)	504 (16%)	3,097
Ticket Fraud	2,905 (95%)	2,168 (71%)	2,572 (84%)	3,061
Other Consumer Non Investment Fraud	2,151 (82%)	1,201 (46%)	1,868 (71%)	2,634
Lender Loan Fraud	1,750 (69%)	669 (26%)	1,434 (56%)	2,542
Abuse of Position of Trust	532 (29%)	124 (7%)	447 (24%)	1,844
Other Financial Investment	1,041 (64%)	406 (25%)	886 (54%)	1,636
Corporate Employee Fraud	494 (34%)	70 (5%)	460 (32%)	1,447
Application Fraud (excluding Mortgages)	718 (53%)	604 (44%)	147 (11%)	1,366
Rental Fraud	1,173 (89%)	923 (70%)	943 (72%)	1,312
Door to Door Sales and Bogus Tradesmen	662 (66%)	213 (21%)	609 (61%)	1,006
Insurance Related Fraud	89 (9%)	39 (4%)	59 (6%)	951
Dating Scam	722 (100%)*	565 (78%)	409 (57%)	722
Lottery Scams	97 (16%)	30 (5%)	76 (12%)	610
Counterfeit Cashiers Cheques	395 (81%)	368 (76%)	106 (22%)	487
Consumer Phone Fraud	139 (29%)	111 (23%)	43 (9%)	478
Insurance Broker Fraud	65 (14%)	30 (7%)	60 (13%)	454
Share sales or Boiler Room Fraud	75 (28%)	18 (7%)	68 (25%)	272
Business Trading Fraud	183 (75%)	127 (52%)	68 (28%)	243
Telecom Industry Fraud (Misuse of Contracts)	22 (10%)	5 (2%)	19 (8%)	229
False Accounting	47 (21%)	19 (8%)	37 (16%)	225
Fraudulent Applications for Grants from Government Organisations	208 (93%)	6 (3%)	205 (92%)	224
Other Regulatory Fraud	129 (62%)	97 (47%)	90 (43%)	208
Fraud Recovery	102 (50%)	12 (6%)	97 (47%)	205
Inheritance Fraud	40 (20%)	23 (11%)	32 (16%)	204
“419” Advance Fee Fraud	93 (55%)	54 (32%)	74 (44%)	169
Fraud by Failing to Disclose Information	75 (51%)	41 (28%)	57 (39%)	148
Charity Fraud	58 (61%)	30 (32%)	42 (44%)	95
Corporate Procurement Fraud	14 (16%)	5 (6%)	9 (10%)	89
Pension Fraud committed on Pensioners	16 (21%)	7 (9%)	11 (15%)	75
Pyramid or Ponzi Schemes	41 (55%)	31 (42%)	17 (23%)	74
HM Revenue and Customs Fraud (HMRC)	3 (4%)	0	3 (4%)	72
Time Shares and Holiday Club Fraud	55 (86%)	31 (48%)	49 (77%)	64
Pension Liberation Fraud	14 (24%)	8 (14%)	6 (10%)	58
Mortgage Related Fraud	19 (35%)	1 (2%)	18 (33%)	55
Fraudulent Applications for Grants from Charities	28 (70%)	20 (50%)	15 (38%)	40
Dishonestly retaining a wrongful credit	17 (77%)	3 (14%)	17 (77%)	22
Bankruptcy and Insolvency	2 (11%)	1 (6%)	2 (11%)	18
Prime Bank Guarantees	14 (82%)	6 (35%)	13 (76%)	17
Passport Application Fraud	1 (11%)	1 (11%)	1 (11%)	9
DVLA Driver Licence Application Fraud	3 (60%)	3 (60%)	1 (20%)	5
Department of Works and Pensions (DWP) Fraud	2 (67%)	1 (22%)	1 (33%)	3
Pension Fraud by Pensioners (or their Estate)	1 (100%)	0	1 (100%)	1
Total	**44,614 (69%)**	**28,190 (43%)**	**32,107 (50%)**	**64,857**

* Categories of fraud assumed in the analysis to be cyber-enabled.

Analysis of victim/offender location (police force areas)

TABLE C3: A breakdown of allocated crimes in which the suspected offender and victim address are in the same police force area, by fraud category (see Figure 8, p24).

Fraud category	Same police force area	%	Different police force area	%	Total
Corporate Employee Fraud	511	55.6	408	44.4	919
False Accounting	54	54.5	45	45.5	99
Abuse of Position of Trust	469	54.5	391	45.5	860
Other Regulatory Fraud	23	53.5	20	46.5	43
Corporate Procurement Fraud	23	52.3	21	47.7	44
Bankruptcy and Insolvency*	5	50.0	5	50.0	10
Fraudulent Applications for Grants from Charities	10	47.6	11	52.4	21
Retail Fraud	927	44.6	1151	55.4	2078
Mortgage Related Fraud	10	37.0	17	63.0	27
Door to Door Sales and Bogus Tradesmen	116	35.5	211	64.5	327
Fraud by Failing to Disclose Information	19	32.8	39	67.2	58
Rental Fraud	173	31.9	369	68.1	542
“419” Advance Fee Fraud	7	31.8	15	68.2	22
Application Fraud (excluding Mortgages)	76	27.9	196	72.1	272
Inheritance Fraud	3	25.0	9	75.0	12
Charity Fraud	9	25.0	27	75.0	36
Insurance Broker Fraud	6	25.0	18	75.0	24
Dating Scam	28	20.6	108	79.4	136
Mandate Fraud	43	19.4	179	80.6	222
Ticket Fraud	103	18.6	452	81.4	555
Other Fraud (Not covered elsewhere)	318	17.2	1526	82.8	1844
Time Shares and Holiday Club Fraud	3	16.7	15	83.3	18
Dishonestly retaining a wrongful credit*	1	16.7	5	83.3	6
Other Financial Investment	85	15.6	461	84.4	546
Other Consumer Non Investment Fraud	145	15.3	800	84.7	945
Pension Liberation Fraud	5	15.2	28	84.8	33
Other Advance Fee Frauds	105	14.0	643	86.0	748
Consumer Phone Fraud	2	13.3	13	86.7	15
Cheque, Plastic Card and Online Bank Accounts (not PSP)	155	13.1	1032	86.9	1187
Pyramid or Ponzi Schemes	3	13.0	20	87.0	23
Pension Fraud committed on Pensioners	4	12.1	29	87.9	33
Lender Loan Fraud	15	11.7	113	88.3	128
Share sales or Boiler Room Fraud	13	9.4	125	90.6	138
Business Trading Fraud	9	8.3	99	91.7	108
Fraud Recovery	5	8.2	56	91.8	61
Lottery Scams	2	7.7	24	92.3	26
Online Shopping and Auctions	298	6.7	4119	93.3	4417
Telecom Industry Fraud (Misuse of Contracts)	9	6.6	128	93.4	137
Insurance Related Fraud	2	4.5	42	95.5	44
Counterfeit Cashiers Cheques	12	4.5	257	95.5	269
Computer Software Service Fraud	4	4.3	88	95.7	92
Fraudulent Applications for Grants from Government Organisations	6	4.3	135	95.7	141
Passport Application Fraud*	0	0.0	3	100.0	3
HM Revenue and Customs Fraud (HMRC)*	0	0.0	3	100.0	3
Pension Fraud by Pensioners (or their Estate)*	0	0.0	1	100.0	1
DVLA Driver Licence Application Fraud*	0	0.0	2	100.0	2
Prime Bank Guarantees*	0	0.0	2	100.0	2
Department of Works and Pensions (DWP) Fraud*	0	0.0	0	0.0	0
Grand Total	**3816**	**22.1 1**	**3461**	**77.9**	**17277**

* All offence categories with a total volume of 10 or less were excluded from Figure 8 in the main report.

Vulnerability and impact analyses

The 48 categories used by the police to classify recorded fraud were reduced to 25 for the purposes of analysing victim impact and vulnerability (see Table C4). All fraud-types which comprised less than 0.5 per cent of the total number of frauds (n=64,857) allocated in 2016-17, were combined with others of a most similar type; for example, specific investments frauds recorded by the police each comprised less than 0.5 per cent of the total sample and were combined to formulate 'Investment fraud categories'.

TABLE C4: A breakdown of the allocated crimes for the analysis of each victim's self-reported and vulnerability (see Figure 9, p26 and Figure 10, p27).

No.	Fraud categories	% of total allocated fraud
1	Retail fraud	4.82%
2	Insurance broker fraud	0.70%
3	**Charity fraud**	
	Fraudulent applications for grants from government organisations	0.35%
	Charity fraud	0.15%
	Fraudulent applications for grants from charities	0.06%
4	Insurance related fraud	1.47%
5	Corporate employee fraud	2.23%
6	Cheque, plastic card and online bank accounts (not PSP)	6.10%
7	Lottery fraud	0.94%
8	**Business fraud**	
	Business trading fraud	0.37%
	Telecom industry fraud (misuse of contracts)	0.35%
	False accounting	0.35%
	Other regulatory fraud	0.32%
	Fraud by failing to disclose information	0.23%
	Corporate procurement fraud	0.14%
	Bankruptcy and insolvency	0.03%
9	**Investment fraud categories**	
	Share sales or boiler room fraud	0.42%
	Pyramid or Ponzi schemes	0.11%
	Time shares and holiday club fraud	0.10%
	Prime bank guarantees	0.03%
10	Ticket fraud	4.72%
11	Counterfeit cashiers cheques	0.75%
12	Application fraud	
	Application fraud (excluding mortgages)	2.11%
	Mortgage related fraud	0.08%
	Dishonestly retaining a wrongful credit	0.03%
13	Mandate fraud	5.82%
14	Online shopping and auction fraud	21.41%
15	Rental fraud	2.02%
16	Door to door sales and bogus tradesmen	1.55%
17	**Other advance fee fraud**	
	Other advance fee frauds	9.68%
	Fraud recovery	0.32%
	Inheritance fraud	0.31%
	"419" advance fee fraud	0.26%

No.	Fraud categories	% of total allocated fraud
18	Other consumer non investment fraud	4.06%
19	Fraud by abuse of position of trust	2.84%
20	Computer software service fraud	4.78%
21	Consumer phone fraud	0.74%
22	Other financial investment fraud	2.52%
23	**Other fraud**	
	Other fraud (not covered elsewhere)	11.36%
	Pension fraud committed on pensioners	0.12%
	Pension liberation fraud	0.09%
	Pension fraud by pensioners (or their estate)	0.00%
	HM Revenue and Customs fraud (HMRC)	0.11%
	Passport application fraud	0.01%
	DVLA driver licence application fraud	0.01%
	Department of Works and Pensions fraud	0.00%
24	Lender loan fraud	3.92%
25	Dating fraud	1.11%

The Police Foundation
The Foundry
17 Oval Way
Kennington
London SE11 5RR
020 3752 5630

www.police-foundation.org.uk

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank