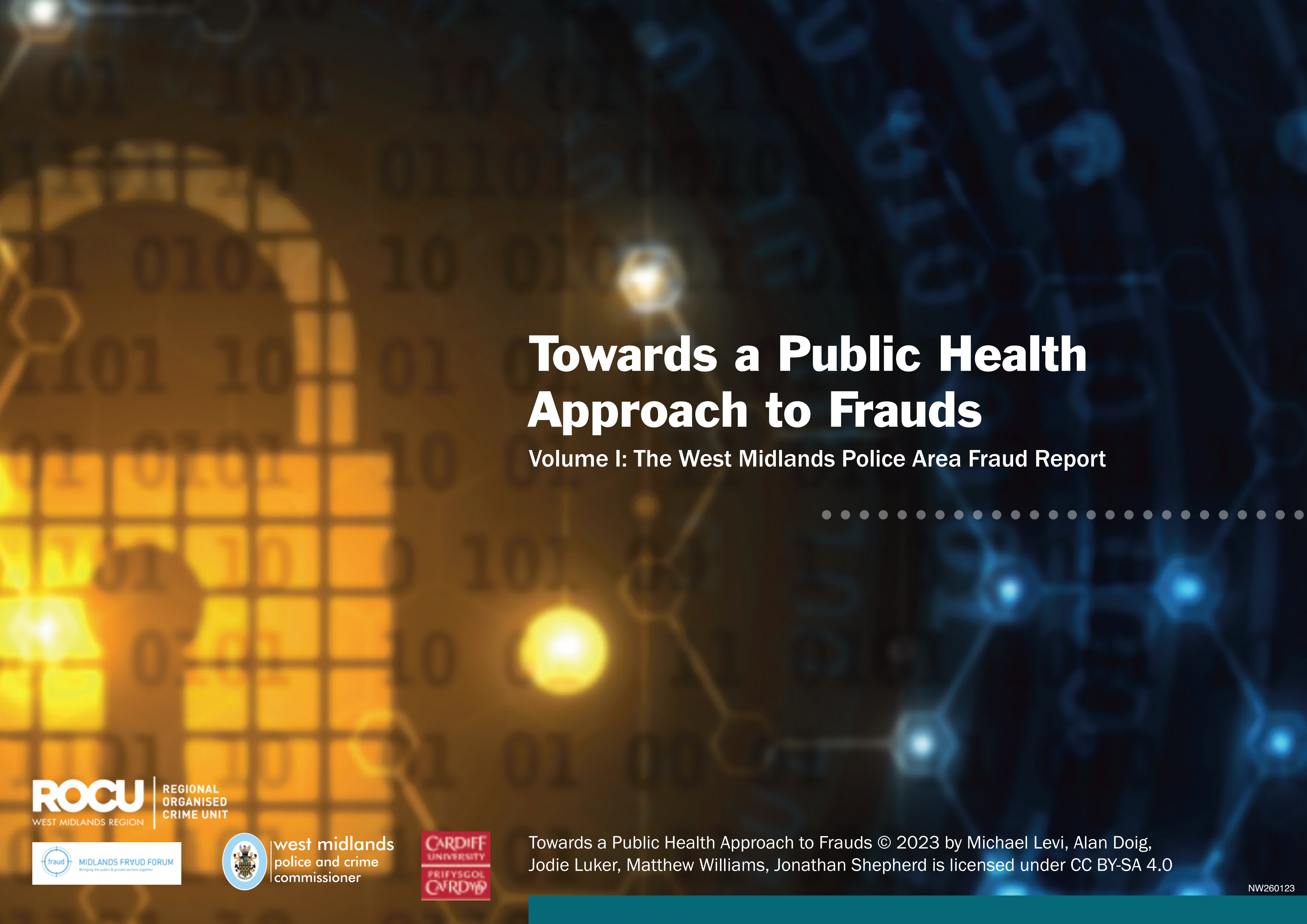


Towards a Public Health Approach to Frauds

Volume I: The West Midlands Police Area Fraud Report

ROCU REGIONAL ORGANISED CRIME UNIT
WEST MIDLANDS REGION

MIDLANDS FRAUD FORUM

west midlands police and crime commissioner

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

NW260123

Foreword

I welcome the report: “Towards a Public Health Approach to Frauds” as an important contribution to the prevention and tackling of fraud. Globally, nationally and regionally, there has been a collective failure to get a grip on fraud, notwithstanding that it is the crime type most likely to be experienced by a member of the public in the UK. Fraud now makes up 40% of all crime, most of which is cyber enabled and it is costing individuals and businesses £4.7 billion each year.

It is widely accepted that the UK’s response to fraud is inadequate. The national response to fraud and cybercrime too often lacks coordination and is failing victims. That is a failure on the part of government to comply with its duty to keep people safe and secure. In order to seek access to justice, victims are required to navigate a complex legal landscape, without any clear expectation of the outcome.

On 18th October 2022, the all party House of Commons Justice Committee called on the Government to:

“…revolutionise the way in which we fight fraud, ensuring it is given greater priority and resourcing across the justice sector to boost prevention, investigation and prosecution alongside improving the treatment for victims of this crime.”

There is a clear need for an end to end overhaul of the way fraud is dealt with, throughout our criminal justice system. Fraud is a national issue and that requires an effective national response, commensurate with the level of threat, risk, harm, demand, need and vulnerability.

We need robust policing and enforcement to tackle fraud. However, we also need prevention and partnership. Prevention, because the prevention of fraud will always be better than having to deal with the consequences of fraud. Partnership, because we need collaboration and joint working, globally, nationally and regionally, within the public and private sectors and across the entire spectrum of the criminal justice system, because policing cannot tackle fraud on its own.

That is why, my Office and I have undertaken an extensive and wide-ranging exercise, assessing how communities and local partnerships can effectively tackle fraud in the West Midlands. That has included, actively seeking to develop an innovative, public health approach to fraud, that focuses on prevention and partnership.

We commissioned a viability and recommendations study by Professors Michael Levi, Alan Doig and Jonathan Shepherd, at Cardiff University on the possibility of implementing a public health approach to fraud. I commend and thank the authors, who have worked tirelessly to prepare this Report. We now have “Towards a Public Health Approach to Frauds” that includes a series of 8 Recommendations on how to implement a public health approach to fraud in the West Midlands.

I invite policing and wider criminal justice partners to consider the Report and in particular the Recommendations set out in the Report. They are as equally applicable to other police force areas, as they are to the West Midlands. It will be my intention to work with partners, with the aim of implementing the Recommendations, to collectively and collaboratively do what it takes to prevent and tackle fraud.

Simon Foster
West Midlands Police and Crime Commissioner

Acknowledgments and Preface

Developing a perspective that presents the victims' and local police force's eye view of fraud and what a public health approach to fraud might be like has been a challenging task far beyond what was originally envisaged. Our primary thanks are due to the West Midlands Office for Police and Crime Commissioner, not just for commissioning this work but for their ongoing engagement with the issues. The PCC, the West Midlands Regional Organised Crime Unit, and the Midlands Fraud Forum co-funded this study, for which we are grateful.

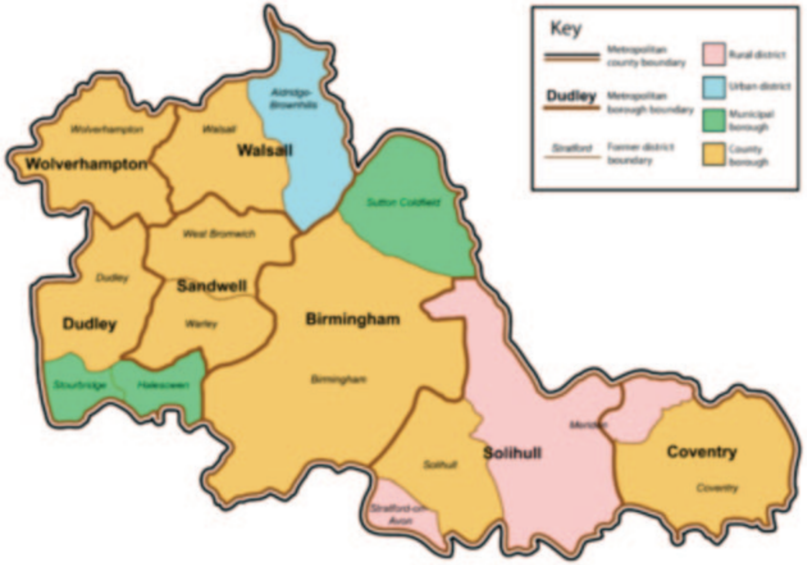
Brendan Warner-Southwell has been an excellent intermediary, and has helped us sustain our interest; Former Deputy PCC Waheed Saleem and his successor Wasim Ali have encouraged and kept us to task throughout the process; Wayne Haynes, formerly of the West Midlands Regional Organised Crime Unit,was the crucial conduit for the data we needed to analyse and an invaluable source of insight into that data; Kuldeep Maan and Christopher King of Dudley Trading Standards convinced us with evidence that they were doing fine work; and Alex Pritchard and colleagues gave us a thoughtful assessment of the challenges the West Midlands police face in managing frauds. We are also grateful for insights from staff at the City of London police, the National Crime Agency, the National Cyber Security Centre, the Serious Fraud Office, National Trading Standards, the MASH teams, and to Andrew Passenger of Carmarthenshire Trading Standards.

This has been a period of unprecedented urgency in policy responses to the now acknowledged large and growing problem of some forms of fraud. We hope that these detailed reports will assist in keeping policies and practices grounded in the complexities of the routine as well as of the exotic and emotive frauds that excite the mass media. These are very tough 'wiki' social problems and they require both central and local responses from police and non-police agencies and the private and third sector alike. Those responses will take time to mature and will be found in actions on the ground rather than in policies alone.

List of Acronyms

ACCC	Australian Competition and Consumer Commission
AF	Action Fraud
APP	Authorised Push Payment
APCC	Association of Police and Crime Commissioners
B	Birmingham
BEIS	Business, Energy and Industrial Strategy department
BID	Business Improvement Districts
BT	British Telecom
CCG	Clinical Commissioning Group
CJS	Criminal Justice System
CPS	Crown Prosecution Service
CRM	Contingent Reimbursement Model
CRN	Crime Reference Number
CSEW	Crime Survey for England and Wales
CV	Coventry
DofE	Department of Education
DPP	Director of Public Prosecutions
DY	Dudley
ECU	Economic Crime Unit
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority
FoS	Financial Ombudsman Scheme
FSCS	Financial Services Compensation Scheme
FTE	Full-Time Equivalent
GP	General Practitioner
HM	His Majesty
HMRC	HM Revenue and Customs
ICO	Information Commissioner’s Office
ISP	Internet Service Provider
MaPS	Money and Pensions Service
MAT	Multi Academy Trusts
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NECC	National Economic Crime Centre
NECVCU	National Economic Crime Victim Care Unit
NFA	National Fraud Authority
NFIB	National Fraud Intelligence Bureau
NHS	National Health Service
NTS	National Trading Standards
OCG	Organised Crime Group
OFT	Office of Fair Trading
ONS	Office of National Statistics
P2P	Person to Person
PBX	Private Branch Exchange
PCC	Police and Crime Commissioners
PND	Police National Database
PSP	Payment Service Provider
Q	Quarter
RART	Regional Asset Recovery Team
ROCU	Regional Organised Crime Unit
SFO	Serious Fraud Office
SIM	Subscriber Identity Module
SME	Small to Medium Enterprise
SNA	Social Network Analysis
UK	United Kingdom
US	United States
WM	West Midlands
WMOPCC	West Midlands Office of the Police and Crime Commissioner
WMP	West Midlands Police
WS	Walsall
WV	Wolverhampton

West Midlands Area



https://en.wikipedia.org/wiki/West_Midlands_%28county%29

Contents

OVERVIEW, RECOMMENDATIONS and EXECUTIVE SUMMARY

PART A. INTRODUCTION

PART B. THE DATA: REPORTS OF FRAUD FOR THE WMP AREA, MAY 2020 TO JULY 2021

PART C. DISCUSSION: DATA ISSUES AND DATA FINDINGS

PART D. DEVELOPING A PUBLIC HEALTH APPROACH TO FRAUDS

Contents

ANNEXES, BOXES, FIGURES AND TABLES

Overview, Recommendations and Executive Summary

OVERVIEW

There is a significant risk that people In England and Wales will become victims of frauds[1] – around 1 in 12 people annually (plus 1 in 33 people for computer misuse offences like hacking): considerably more in our lifetimes. Frauds in the aggregate continue to rise, and – if left to their own devices - may be expected to rise further as inflation and economic pressures incline more people to look for innovative ways to pay their bills and to try to find savings and investments that claim to beat inflation. Although many offenders will not be local, fraud's impacts are felt in our homes and families and even when people become victims via the smartphone and Internet, it may properly be characterised as 'neighbourhood crime'. However, in aggregate (though very seldom individually) it is also arguably a collective threat to our national and human security. In the context of other demands on policing such as dealing with violent crimes in the home and on the streets, however, fraud still occupies a subsidiary spot in the minds of the public as well as in the minds (and effective caseload) of the police. The key concerns with maintaining the current status quo are: declining public confidence in the police; gaps in service for the majority of victims, including those who want/need a service – plus information (as well as resource) gaps in the challenges of identifying and intervening against repeat victimisation; practical barriers to resourcing and implementing greater responses from within the criminal justice system; and challenges of addressing fraud at a local and regional level, irrespective of broader changes at the national level, whether to private, public or third sectors (e.g. charities).

At the request of the West Midlands Office of the Police and Crime Commissioner (WMOPCC) we have reviewed the wider fraud context: *Volume II: the Background Report*. This provided us with the context to analyse over a year's worth of Action Fraud (AF) and other data relating to the West Midlands Police (WMP) for this volume: *Volume I: the West Midlands Area Fraud Report*. The purpose has been to consider whether a public health approach could add value to responses to fraud in the West Midlands. We are aware that the conceptual thinking behind such an approach will require a strong shift towards building up personal and third party defences against frauds, and this will take time. It may require that organisations other than the police will take primary responsibility on a coordinated and resourced basis for encouraging people to use the internet safely and avoid dangerous activities. On the other hand, there are important concerns about both police responses and fraud prevention, and a public health approach may offer more positive and more effective responses to those concerns. In doing so, we will only make a limited number of recommendations to operationalise a public health approach adapted for fraud. Our starting point for a realistic public health response is that most current and future victims of fraud are unlikely to receive significant support and care, even if their case is triaged by the National Fraud Intelligence Bureau (NFIB) for dissemination to the West Midlands Police (WMP). Nor will many 'ordinary' fraud victims receive much assistance from the National Crime Agency which, understandably in the light of its remit, is focused on those 'high harm' offenders – a proportion of whom are engaged in frauds of varying kinds – who meet its threshold for Serious and Organised Crime.

This Report is divided into 4 PARTS. These are: [PART A] an introduction to WMP, to fraud statistics headlines and to adapting/developing a public health approach to reduce the levels of fraud through prevention; [PART B] an analysis and interpretation of AF data – using a range of variables, cross-referenced by postcode before being measured against current national data, AF data from 2014 and Disseminations data; [PART C] discusses what the findings say about fraud in the WMP area and their relevance for adapting or developing a public health approach; and [PART D] concludes with a discussion of issues or constraints on a public health approach, assessing how far that approach may be developed within the context of the 4 Ps – Prevent, Protect, Prepare and Pursue – used by government and law enforcement as a strategic framework within which

[1] From the outset – and why we use the plural term 'frauds' in the Report title. We consider that fraud is not a homogeneous form of behaviour (and that it might be preferable to use the plural term 'frauds' to emphasise that variation). The fraudster population is varied, from Organised crime groups (OCGs) increasingly moving into parts of fraud, insider and outsider opportunists, professional specialists at home and overseas or both, etc...

Thus, between the 'high policing' of serious or complex fraud by the Serious Fraud Office (SFO) and the 'organised crime' policing of frauds committed by OCGs, there is a large hinterland of fraud, from non-trivial (though non-OCG) to volume or lower-value fraud, that did not appear to be any enforcement agency's specified business (or, when it was, could still end up being filtered out or into a major investigation). Further, what may prevent or discourage fraudsters is varied; there is at present no one reason why any of them would stop of their own accord if they were not convicted, not shamed in ways they considered relevant or not deflected or incapacitated via prevention efforts, whether or not those efforts occurred via the criminal justice system.

to address serious and organised crimes (e.g. via the National Economic Crime Centre's national co-ordinating role), and finally proposing recommendations on a public health approach to fraud.

In the light of the confidential nature of the data, most of the tables, charts and other statistical material, as well as some of the narrative provided with the data, have been made available in confidence to the WMOPCC in an expanded version of this Report. The data and other materials in this edited report are approved for public dissemination by the WMOPCC.

RECOMMENDATIONS

1. RECOMMENDATION 1: Central to reform is the recommendation that the WMOPCC formally takes ownership and coordination of the approach. This is necessary (a) to bring together all relevant organisations and expertise, and (b) to make strategic and financial decisions appropriate to the level and type of intervention. For any initiative based on the Action Fraud (AF) data in terms of victims' volume of fraud, median loss, age, ethnicity, repeat victimisation and postcode, the WMOPCC needs to pull together the three groupings discussed in the Report to assess current work and overlaps; appetite for engagement; initiatives elsewhere that may be applied to the WMP Area; and enthusiasm for working together on a prevention strategy. 'Buy in' – both financial and in energetic support - from key stakeholders on a modest number of initiatives is needed to deliver a holistic public health approach in practice: it will evolve over time.

   Without pre-empting their choices, the organisations involved should assess potential initiatives to determine levels of engagement, resources, added-value and evaluations of impacts. Given how high repeat victimisation currently is, we recommend a general focus on reducing this, which requires some prior specialist knowledge of and interest in fraud/scams, since these differ from other forms of repeat victimisation such as burglary and violent crime. We propose 7 possible short-term interventions (Recommendation 2 to 8 below).

2. RECOMMENDATION 2: for the high-volume fraud categories, we recommend a 'statement of intent' in the form of a public campaign labelled specifically as being for the WM Area involving financial services institutions, including existing information and campaigns on risk, and awareness and guidance, as well as a crafted message underlining what the police currently can and cannot do in the event of a fraud.

3. RECOMMENDATION 3: we recommend targeted tertiary interventions where repeat victims might raise their concerns – Citizens Advice Bureaux, doctors' surgeries, social care companies, community and youth groups such as Age Concern, Saga, Guides, Scouts, Youth Clubs, sports teams, and so on. These and other organisations, such as the West Midlands Clinical Commissioning Groups (CCGs), might help ensure that despite current high demand-supply imbalances, ongoing mental health services are accessible for at least *some* victims of fraud. Conversely, such organisations should have a means to collate and coordinate identified support and supervision for vulnerable or repeat victims. Some particular vulnerabilities – for example, the increasing numbers of people with declining or severe mental capacity problems - may be given special treatment or focus. They are at risk not just from strangers but from family and friends, and even from those purporting to be professionals (such as financial advisors, whether FCA-approved or not).

4. RECOMMENDATION 4: we recommend a primary prevention level approach incorporating fraud and financial literacy awareness within primary and secondary school class modules that already address life skills. Given the rising fraud risks over the lifecycle, cyber-risks (including fraud) should be included in the curriculum, despite strong competition for such inclusion. The secondary prevention benefit is that this might make the group more aware of and armed against scams involving apps and the search for 'bargains'. Appropriate material will have to be researched and evaluated with children, and made available to educational authorities for use within the curriculum. Some training certainly will be needed but we anticipate that many issues will be well-known to existing staff who will deliver the material, after consultation. Such an approach should be pursued, as we suggest above, with any organisation working with young people (including Guides, Scouts, Youth Clubs, sports teams, etc); young people need to be encouraged to assess both probabilities and consequences, in a range of activities including online shopping, online gambling, 'ghost broking' of motor insurance, investments such as crypto-markets and warnings about credulous following of social

media 'influencers' and about lending their bank accounts for money muling.

5. RECOMMENDATION 5: we recommend the proactive engagement of third-party institutions in targeted campaigns in specific postcodes. Banks are increasingly engaged in alerting victims – especially those already identified as 'vulnerable' to the risk of making increasing levels of payments, often overseas, in dating and other scams, especially Authorised Push Payment frauds. While some dating websites have inadequate due diligence and validation of clients, we suggest that in conjunction with banks and law enforcement, media and social media campaigns could be undertaken in group or community interventions through ethnic or social community groups proposed for specific NFIB categories and/or postcodes.

6. RECOMMENDATION 6: a multi-agency approach to primary intervention would involve training up those working with people at higher risk to pass on concerns to appropriate agencies. The report has identified the sort of frauds to which the 70+ age group may be particularly vulnerable. The multi-agency initiative would involve those involved in the second initiative, but would also include training medical staff, care workers and family carers, financial institutions, and others to identify signs of stress or distress, or unusual patterns of activity, and to know to whom to report the information, with appropriate response arrangements put in place. This has resource implications both for those potential preventing/reporting staff and for those charged with responding to the reports.

7. RECOMMENDATION 7: we recommend a focus on secondary interventions for smaller businesses, charities and other organisations for frauds that specifically affect them, including employee fraud, procurement fraud and mandate fraud. While these are small in number, potential losses may be high and the collateral harm – loss of employment etc. – greater. Here specialist advice and on-line or telephone hotline advice and support could be provided across a range of organisations by a trusted third party such as the Midlands Fraud Forum, who could draw on its membership for an annual portfolio of seminars and training offered as part of the WM OPCC interventions. This might complement other efforts such as a current initiative of the Fraud Advisory Panel with SMEs.

8. RECOMMENDATION 8: we recommend that consideration be given to a larger (non-standing) capability for reactive investigation of large-scale frauds, alone or in combination with other forces, whether that be via the Association of PCCs, the City of London police, the National Crime Agency and the NECC, expanded economic crime teams within Regional Organised Crime Units, the Serious Fraud Office or some future body created as a response to what is widely acknowledged as the 'fraud policing deficit'. The public health focus should be on prevention, but preparation for corporate compliance/governance deficits on the scale of HBOS/Lloyds Reading needs to be carried out, and if there were several such large scale cases (including crypto/investment frauds) simultaneously or overlapping, it is not clear that England and Wales (let alone the West Midlands police) currently has the capacity and capability to deal with them, given the length of time they take and the resources they consume. This could fall within the original remit of the SFO, but they are not funded currently to carry out this role. We have focused in this Report on the more mundane frauds, but the public in the West Midlands and elsewhere may need reassurance that more can be done (and more quickly) with cases that are not part of 'volume crime' or 'Organised Crime Groups' as conventionally understood. Of course, they may want to see more reactive response to 'local' frauds also, and we support up-skilling of police to deal with these among the many other areas of policing activity. Such thinking is not a conventional part of public health, but within-corporate or within-government 'rotten pockets' can occur in any part of the UK, and whether the harms are localised or are more widely distributed geographically, reducing their *scale* is important.

EXECUTIVE SUMMARY

9. The West Midlands Police (WMP) is the second largest police force in the country, reflecting the size of its population; its fifth largest level of recorded crime is fraud, while less than 1% of WMP's FTE serve in the Economic Crime Unit. Using the latest public Action Fraud (AF) data on referrals and outcomes for fraud and cybercrime broken down by Home Office police forces and other agencies in the UK for 1 April 2019 – 31 March 2020, 37,951 were referred to police forces, of which 6,363 resulted in a judicial outcome. Therefore, the attrition rate for fraud means that 11.6% of AF reports go for investigation and only 16.7% of the referrals result in a judicial outcome – this is 2% of those

reporting a fraud to AF. From the research project's analysis of AF data relating to the WMP, the situation in West Midlands is little different from the country as a whole.

10. There is a significant risk that people will become victims of fraud – currently around 1 in 12 people annually and considerably more over their lifetimes. (This is an addition to tax, benefit and other public sector frauds of which we are victims collectively, but which are out of scope for this report.) It is not yet clear whether the poor criminal justice response to fraud will erode public legitimacy of the police. However, in the context of other demands on policing such as dealing with violent crimes in the home and on the streets, capacities and capabilities fraud has always been a low priority for the police. Preventive interventions with seriously harmed individuals and/or those at high risk of repeat victimisation will be necessary, involving relevant organisations and coordinated through the WMOPCC.

11. In such circumstances, and reflecting the conceptual thinking behind 'public health' and reviewing current approaches to, and concerns about, frauds in our background study – *Volume II: the Background Report* - we proposed in that Report that a public health approach, adapted or developed for the fraud context, would add value to fraud responses but would require a significant but essential shift to prevention. The approach would require organisations other than the police to take up primary responsibility on a coordinated and resourced basis for increasing situational prevention measures for a range of frauds.

12. The point of a public health approach – and not all such approaches are successful - is to consider different intervention points and levels, involving awareness and self-driven prevention – including knowledge from failed attempted frauds - and engagement with partners, businesses, and others to reduce fraud through prevention. As with general and terrorist violence reduction, the public may not even be aware of third party interventions by public or private bodies that reduce their risks, before and after individuals or organisations become victims. Nevertheless, promotion and awareness of the wider picture is important to emphasise the holistic and communitywide nature of the approach. A sharper focus on identifying and helping people who are likely to become repeat victims is also important, both as a good practice in itself to reduce harm that those individuals suffer and also to reduce crime levels.

13. The AF data underscores several points, particularly those that emphasise that fraud is not a homogeneous form of behaviour (which is why it might be better to use the term 'frauds', to emphasise variation); nor are all frauds equally harmful (although harm is not simply economic loss), and nor are they all caused or perpetrated in the same way. Out of the 50 fraud categories and cases recorded by AF over a 14 month period, most of the specified (49) categories of fraud relating to the WMP yield very low levels of reported cases: in the West Midlands, only 5 categories have more than 5% of the total of reported cases, all of which had median losses less than £500. Over 90% of reported cases involve individuals.

14. Some frauds impact more greatly on particular age and ethnic groups; specific groups, such as 70+, are disproportionately represented in particular types of fraud. The analysis showed high levels of repeat victimisation (although the data does not tell us whether this is for the same offence or over what time period). High levels of repeat victimisation are found in some NFIB categories with few cases; others - like NFIB19 (Abuse of Position of Trust) or NFIB5A (non-PSP Cheque, Plastic Card and Online Bank Accounts) – have very many cases. While most cases and median losses are proportionately distributed across the five postcodes in the West Midlands, applying age, ethnic and vulnerability variables against postcodes shows that some groups and frauds stand out as more or as less vulnerable to fraud.

15. AF contemporary data on the volume of cases for the WMP Area is roughly similar to the national picture. On the other hand, comparing the AF WMP data against national data from 2014 shows not only an overall increase in the number of cases but also changes in the relative frequency and severity of particular sorts of fraud. Cases involving NFIB5A (non-PSP Cheque, Plastic Card and Online Bank Accounts) and NFIB5B (Application Fraud excluding Mortgages) have declined proportionally. On the other hand, investments scams, such as Boiler room frauds and Ponzi schemes, have increased. Online shopping fraud has risen strongly. These show that (not only because of Covid-19) the internet has driven increases in some categories, while financial services sector efforts have prevented increases in fraud – in some cases quite significantly. Median losses, however, have decreased in the majority of categories; only in 4 have they

increased, and most of those relate to business rather than individual activity.

16. A review of data for the same period shows that the NFIB disseminated over 1200 reports to WMP for investigation; in 14 fraud categories, no cases were disseminated. 6 categories accounted for some 60% of cases: 2 of those were also among the top 5 AF categories in terms of volume of cases. Of those cases disseminated, over 60% were not pursued on grounds of evidential difficulties; just over 5% were subject to a judicial outcome. In short, it appears that around 10% of reported fraud is likely to be triaged by the NFIB for dissemination and, of these, fewer than 5% will result in some form of 'objective' positive outcome.

17. Overall, less than 1% of all fraud reported to AF is likely to end up being subject to a WMP investigation that leads to a judicial outcome. The criminal justice attrition – affected by low police fraud resources and capabilities – provides ample justification for arguing that the focus must be on prevention and reducing harm and damage, both to victims and to perceptions of how fraud is policed. Even if police investigation resources were far greater (within the West Midlands and in the UK generally) and attrition less, we would still need to focus primarily on prevention.

18. There were data problems that should be resolved if the AF data is to be used in a public health approach – whether the completeness and level of detail provided, or disaggregating category NFIB90 (None of the Above), which records the largest number of reported cases. Similarly, although more for understanding the triaging process, it would be useful to know the reasons who some cases were disseminated and others were not.

19. To use the data for targeted interventions in relation to specific groups, it is clear that there is a nexus between (a) specific groups and postcodes and (b) specific NFIB categories that are a basis for developing a public health approach to addressing those levels and loci of fraud. Indeed, with 42% of AF cases recorded as repeat victims – and several NFIB categories where all are repeat victims, then the case for an initial focus on repeat victimisation is established.

20. The framework we recommend is of prevention-based interventions that have less to do with tackling offenders than an evidence-informed approach that will engage with community organisations, with health professionals, and with the police both for their deterrence role and for, as will be discussed below, the provision of public reassurance that some of their concerns are being paid attention to. This is not an argument against increasing police resources to increase fraud disruption and justice for victims: it is an argument for a broader attack on fraud which will have to be long term, because the general opportunities for fraud will not go away, whatever efforts are made to enhance policing services or to use public-private and private-private partnerships to reduce particular fraud risks and techniques in some areas.

21. We consider that a public health approach would not function effectively within the 4 Ps, (Prevent, Protect, Prepare and Pursue), especially where there is relatively little systematic information about the rationale, choice, extent, forms and balance between the Ps in determining counter-fraud interventions or their effects, particularly not on their effects on levels and/or the organisation of fraud or on crime for gain generally. Adapting many of the current initiatives within the Ps, in particular Protect, (strengthening our protection against fraud), as well as some of the initiatives from overseas, would work better within a public health approach. This is for three reasons. First the approach focusses on the potential victims and their behaviour in terms of promoting generic awareness and due diligence by the potential victims before they become exposed to a potentially fraudulent activity; second, it requires coordination between organisations and a streamlining of messages to ensure they resonate with particular groups or potentially fraudulent activities; and thirdly, there is a credible or trustworthy source, or sources, whose role in advice, guidance and support is known and easily accessible.

Part A - Introduction

Comprises 2 Sections providing an introduction to the WMP, to headline fraud statistics and to adapting or developing a public health approach to reduce the levels of fraud through prevention

Part A - Introduction

1. REPORT OVERVIEW

1.1 The Report

Notwithstanding the significant risk that people will become victims of fraud – currently around 1 in 12 people annually and far more over their lifetimes - in the context of other demands on policing such as dealing with violent crimes in the home and on the streets, fraud still occupies a subsidiary spot as a crime category in the minds of the public as well as in the minds (and effective caseload) of the police. The key concerns about maintaining the current status quo are: declining public confidence in the police; gaps in service for the majority of victims, including counselling, information on the progress or outcome of their case, and possible avenues for recompense, gaps in the challenges of identifying and intervening against repeat victimisation; practical barriers to additional police resourcing and implementing greater responses from within the criminal justice system; and challenges of addressing fraud coherently at a local and regional level.

Addressing such concerns would, however, require a comprehensive and integrated portfolio of initiatives, including addressing victim expectations, the value of personal engagement (especially in dealing with vulnerable victims who have complex needs), the links to other important local services, and the need for targeted prevention, which can be more readily done by local organisations who can adapt to local problems and local demographics.

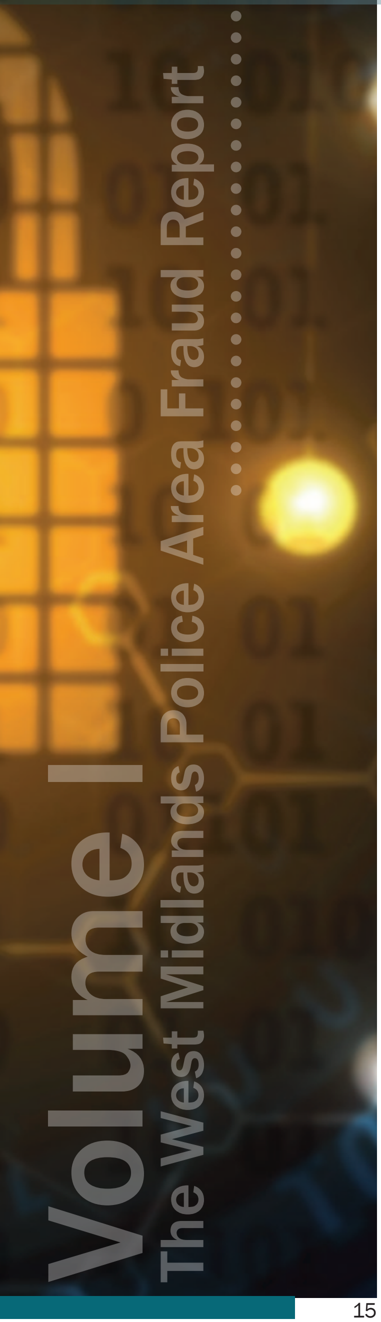
This requires a new way of approaching fraud. Such an approach might dovetail with national-, sector or pan-industry-led initiatives, but could be partly independent of them. To do so would require developing or adapting an appropriate framework within which to propose such initiatives, and a prime candidate is a public health approach will require a strong shift towards building up personal and third-party defences against frauds. It may require that organisations other than the police will take primary responsibility on a coordinated and resourced basis for encouraging people to use the internet safely and avoid dangerous activities, subject to their risk appetite and the consequences of their risky behaviour for others. This is part of the role of the National Cyber Security Centre, but there is a need for a more local dimension.

A public health model could focus more on better protection of potential first time and repeat victims and seek to build up a sense of security and resilience than on discouraging potential offenders (though there is room for research on the latter). Here – noting well-known campaigns around seatbelts and smoking (or even use of mobiles in cinemas) – in addition to warning pop-ups and take-downs of fraudulent promotions as a supply-side approach to fraud control, one key challenge is to regularly warn people in appropriate contexts about the dangers and to nudge potential victims to mentally register their own situation as a potential fraud and identity crime risk.[2]

In terms of harm and engagement with victims, coordinated preventive interventions will need to be both primary (with those in the general population at risk of being defrauded) and secondary (to reduce repeat victimisation). Given the levels of fraud and mechanisms for making the public aware of risks, such interventions will need to be supplemented with a structured, coordinated, and continuing outreach programme by trusted (and trustworthy) organisations and persons. A public health approach seeks to improve general health and safety by modifying underlying risk factors to reduce the likelihood that a person/firm will become a victim or a perpetrator of a crime. This involves a shift towards prevention, broadly conceived, and a shift to where lead responsibilities and the allocation of resources may be most appropriate.

In the light of the current epidemiology of frauds set out in our review of the current fraud context – *Volume II: the Background Report* - we consider that a public health approach is long overdue. The first step is the collection and analysis of available data as an evidence base on which to assess the potential value of public health-type responses/interventions and what forms they should take. We therefore make an initial assessment of fraud data relating to the West Midlands Police (WMP) Area to produce a more informed view of the added-value of such an approach, and to make initial recommendations within a framework informed by a public health public health approach. This involves:

[2] Warnings alone have little impact. See, e.g., Kamar, E., Howell, CJ, Maimon, D. & Berenblum, T. 2022. 'The Moderating Role of Thoughtfully Reflective Decision-Making on the Relationship between Information Security Messages and SMiShing Victimization: An Experiment'. Justice Quarterly, DOI: 10.1080/07418825.2022.2127845.



Part A - Introduction

- collecting and analysing existing data within the West Midlands Police area through Action Fraud (AF), and also those reported fraud data that are then disseminated by the National Fraud Intelligence Bureau (NFIB) to the WMP for action;
- describing and reflecting on the attrition between the reporting of fraud data to AF and outcomes through WMP; and
- making recommendations about what can be done about frauds, by the police and by other bodies if an adapted or developed public health approach is considered and progressed.

In the light of the confidential nature of the data, most of the tables, charts and other statistical material, as well as some of the narrative provided with the data, have been made available only in an expanded report to the West Midlands Office of the Police and Crime Commissioner (WMOPCC). The data and other materials in this edited report are approved for public dissemination by the WMOPCC.

1.2 Summary of Report Structure

This report is divided into 4 PARTS. These provide: [PART A] an introduction to WMP, to fraud statistics headlines and to adapting/developing a public health approach to reduce the levels of fraud through prevention; [PART B] an analysis and interpretation of AF data – using a range of variables, cross-referenced by postcode, before being measured against current national data, AF data from 2014 and National Fraud Intelligence Bureau's (NFIB) Disseminations data; [PART C] discusses what the findings say about fraud in the WMP area and their relevance for adapting or developing a public health approach; and [PART D] concludes with a discussion of issues or constraints on a public health approach (including available data), assessing how far that approach may be developed within the context of the 4 Ps – Prevent, Protect, Prepare, and Pursue - used by government and law enforcement to address serious and organised crimes, and finally proposing recommendations on a public health approach to fraud.

1.3 The WMP Context

WMP is the second largest police force in the country, covering an area of 348 square miles and serving a population of almost 2.8 million. In 2022, West Midlands headquartered nearly 700,000 companies, i.e., almost 8% of all UK companies. The volumes of recorded offences in the year to September 2021 in the WMP are listed in Table 1 (a fuller breakdown of slightly earlier data is given in Box 1). The figure of fraud in Box 1 is provided by the Office of National Statistics (ONS) and has been in recent periods the largest single area of recorded property crime.

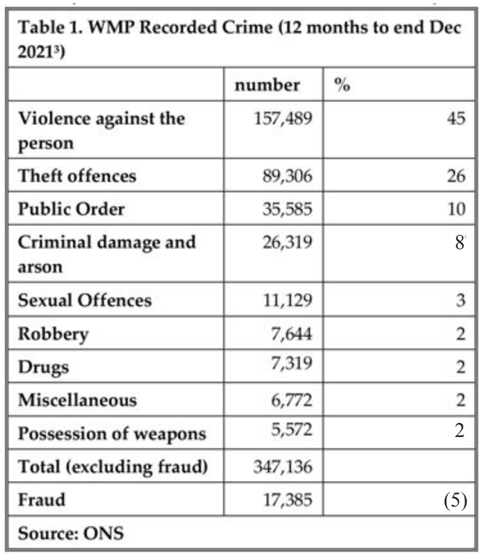


Table 1. WMP Recorded Crime (12 months to end Dec 2021[3])

	number	%
Violence against the person	157,489	45
Theft offences	89,306	26
Public Order	35,585	10
Criminal damage and arson	26,319	8
Sexual Offences	11,129	3
Robbery	7,644	2
Drugs	7,319	2
Miscellaneous	6,772	2
Possession of weapons	5,572	2
Total (excluding fraud)	347,136	
Fraud	17,385	(5)

Source: ONS

Overall, 5% of WMP area crime is fraud-related, while the staffing levels (FTEs) are shown in Table 2 (albeit it is important to note that, overall those levels have decreased in the past decade by over 15%[4]). Of these, 0.65% of WMP's FTE serve in the Economic Crime Unit (where even here some resource, such as financial investigation and asset recovery, may also be deployed for the acquisitive element of non-fraud crimes). This percentage reflects national averages (see Annex 1: WMP Staffing and National Figures).

As we noted in the context study – *Volume II: the Background Study* – we consider that a public health approach offers a fresh way of addressing a range of frauds, and one that allows the police to focus on where their competences and techniques are best deployed. This would be appropriate even if the police had the resource that reflected the level of harmful criminality that frauds represent.

[3] Statistics taken for approximate period covered by fraud data.
[4] See Home Office. 2010. Home Office Statistical Bulletin 14/10: police service strength. London: Home Office.

Part A - Introduction

In considering using a public health approach framework, we are looking at all the identifiable ‘fraud health’ problems in the population as reported by the public and organisations, disaggregated as far as possible by available variables like age and ethnicity. Though the vast majority of frauds that are identified as such remain unreported, we will also consider the NFIB data which are disseminated to WMP as identifiable proxy ‘health’ problems chosen for treatment - the equivalent of Accident & Emergency admissions that have been triaged for treatment/action/no further action – and therefore secondary to the main focus of this Report.

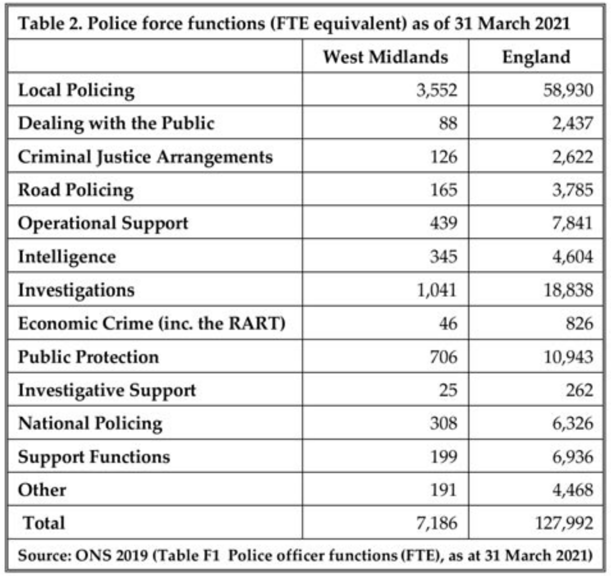
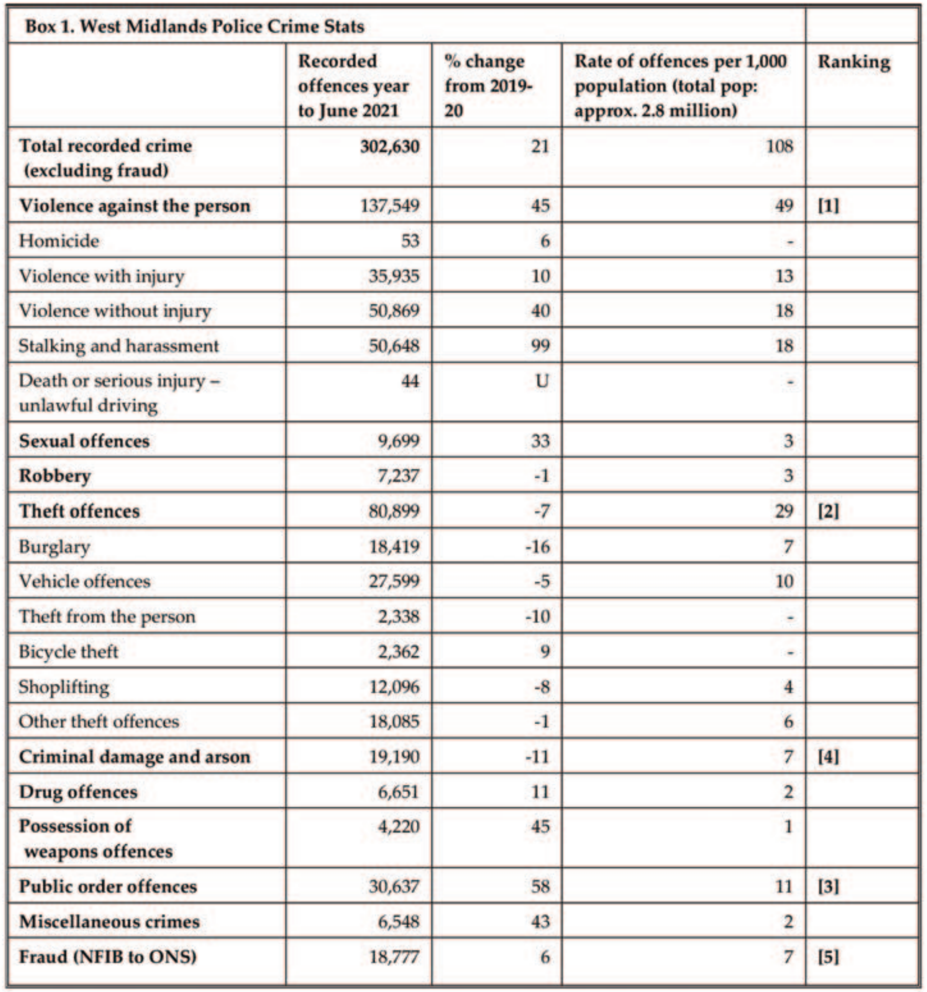


Table 2. Police force functions (FTE equivalent) as of 31 March 2021

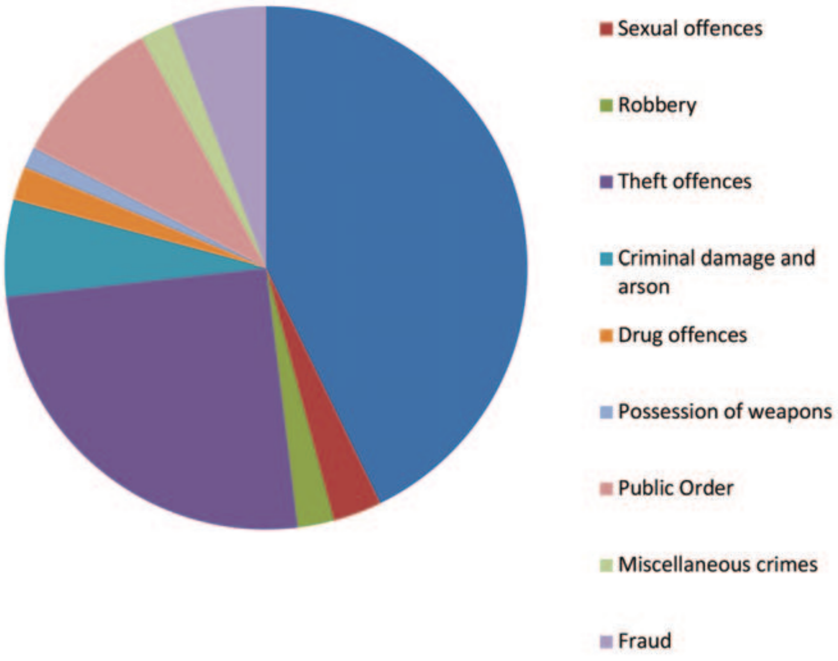
	West Midlands	England
Local Policing	3,552	58,930
Dealing with the Public	88	2,437
Criminal Justice Arrangements	126	2,622
Road Policing	165	3,785
Operational Support	439	7,841
Intelligence	345	4,604
Investigations	1,041	18,838
Economic Crime (inc. the RART)	46	826
Public Protection	706	10,943
Investigative Support	25	262
National Policing	308	6,326
Support Functions	199	6,936
Other	191	4,468
Total	7,186	127,992

Source: ONS 2019 (Table F1 Police officer functions (FTE), as at 31 March 2021)

Part A - Introduction



Box 1. West Midlands Police Crime Stats				
	Recorded offences year to June 2021	% change from 2019-20	Rate of offences per 1,000 population (total pop: approx. 2.8 million)	Ranking
Total recorded crime (excluding fraud)	**302,630**	21	108	
Violence against the person	137,549	45	49	[1]
Homicide	53	6	-	
Violence with injury	35,935	10	13	
Violence without injury	50,869	40	18	
Stalking and harassment	50,648	99	18	
Death or serious injury – unlawful driving	44	U	-	
Sexual offences	9,699	33	3	
Robbery	7,237	-1	3	
Theft offences	80,899	-7	29	[2]
Burglary	18,419	-16	7	
Vehicle offences	27,599	-5	10	
Theft from the person	2,338	-10	-	
Bicycle theft	2,362	9	-	
Shoplifting	12,096	-8	4	
Other theft offences	18,085	-1	6	
Criminal damage and arson	19,190	-11	7	[4]
Drug offences	6,651	11	2	
Possession of weapons offences	4,220	45	1	
Public order offences	30,637	58	11	[3]
Miscellaneous crimes	6,548	43	2	
Fraud (NFIB to ONS)	18,777	6	7	[5]



1.4 The Justice Attrition Rates

In *Volume II: the Background Report* we noted that, compared with the estimated scale of fraud reported as perpetrated in England and Wales, the number of cases reported to Action Fraud (AF) is modest. The number disseminated by the NFIB for a police 'pursue' (e.g. possible investigation and charging) response is even lower. Although we do not have data on their objectives when reporting or on their satisfaction levels after doing so, it is plausible that many victims – the vast majority – may feel that they received a poor service and have been denied justice or an expected outcome.

Earlier research found that while there were over three million cases against individuals each year (as measured then by the CSEW), only around 260,000 (a twelfth) were reported to AF (although we have no accessible data on victims who decide not to report their allegations, or why). Of those who do report, on average, only 27 per cent are disseminated to police forces for an investigation and just three per cent ended with a judicial outcome. So, whatever benefits a criminal justice outcome may or may not bring, depending on the level of victim support, most are unlikely to receive restorative justice, harm mitigation (including their money back) or significant assistance on reducing future victimisation.

We have developed an AF dataset which shows over 20,000 reports of fraud from May 2020 to June 2021. We have also developed another dataset of NFIB Disseminations of over 1,000 reports of fraud for investigation by the West Midlands Police (WMP) between 1st April 2020 and 31st March 2021. Of these latter, fewer than 10% resulted in a judicial outcome to date - and half of those outcomes resulted in suspects being charged or summonsed. No further action was taken in over three-quarters of the reports, largely because of evidential issues. Just over 13% of cases were still pending.

Put another way, using the latest public AF data on referrals and outcomes for fraud and cybercrime broken down by Home Office police forces and other agencies in the UK for 1 April 2019 - 31 March 2020, 37,951 were referred to police forces, of which 6,363 resulted in a judicial outcome. In other words, the fraud attrition rate reveals that 11.6% of AF reports go for investigation and only 16.7% of the referrals result in a judicial outcome – 2% of those reporting a fraud to AF. Thus, the WMP picture is little different from the national picture and, with reports to AF already up 27% 2021-22 on 2019-2020, there is little reason to suppose that the picture will improve 'naturally' for the vast majority of those reporting fraud.

1.5 The Basis for Considering a Public Health Approach?

In 'fraud health' terms, the much larger set of cases reported to AF is essentially those cases being reported by victims because of their desire for some form of law enforcement 'treatment' (or why would they report?). However, only some are chosen for taking forwards after processing and disseminating by the NFIB (which also integrates cases from other sources - see *Volume II: the Background Report* for a fuller explanation). If the Disseminations data represents a proxy for those cases successfully triaged by the NFIB as appropriate and realistic for criminal justice to take on, then some 90% of those reporting 'fraud ill-health' will not be selected for professional help of any kind, beyond receiving generic fraud prevention advice by email or post. Given that this percentage is not unusual, it is important to explore what the data tells us about the types of fraud that are not selected for criminal justice and whether there is room for a greater focus on support, awareness and prevention to reduce the level of 'unsuccessful' reporting and harm. This – as we will discuss below – is particularly relevant for repeat victims and reducing demand for – or expectations of - a law enforcement response.

In terms of harm and engagement with victims, coordinated preventative interventions will need to be considered very seriously, particularly but not only if the resource for the 'pursue' function continues to be very modest. There is a temptation to assume some past Golden Age in which reactive policing of fraud was sufficiently resourced. This has never been the case outside of – arguably – social security benefit fraud, though fraud policing resources were less strained 30 years ago, when volume fraud was very much lower and general police staffing numbers were higher.[5]

In such circumstances, and reflecting the conceptual thinking behind a public health approach, we proposed in *Volume II: the Background*

[5] Levi, M. 1993. The Investigation, Prosecution, and Trial of Serious Fraud. Royal Commission on Criminal Justice Research Study No.14. London: HMSO; Doig, A., Johnson, S., and Levi, M. 2001. 'New public management, old populism and the policing of fraud'. Public Policy and Administration 16(1). pp91-113.

Report that such an approach requires a significant but essential shift to prevention. Except where the police are demonstrably more appropriate, organisations other than the police may be funded to take primary responsibility for encouraging and helping people to use the internet safely and avoid dangerous activities. This will plausibly focus more on protecting the victims than on discouraging potential offenders, and on seeking to build up a sense of security and resilience. Here – notwithstanding well-known campaigns around seatbelts and smoking (or even use of mobiles in cinemas) – the challenge would be not just to warn people about the dangers but to focus on helping potential victims to become 'fraud conscious' or 'fraud alert' in carrying out any transaction, particularly online. The intention is to provide an evidenced platform from which to improve the general 'fraud' welfare of the population, and not just to help the far lesser number of fraud victims whose cases are reported to, or enter, the criminal justice process (and whose satisfaction levels have not been measured properly if at all).[6]

In adapting or developing a public health approach we are aware that not all such approaches are successful and that the approach would not be about care per se but about care designed to prevent future harm. Thus, this Report is not significantly about police performance, constrained as the police are by NFIB dissemination and their own resources, but about the cases they do not see because they have not been triaged by the NFIB,[7] and to recommend interventions to prevent individuals and organisations becoming first-time victims or repeat victims of fraud. It would be interesting to see what fraud victims whose reports are not followed through think about the system, but this modest project has no capacity to examine it. However, both in prosecuted and unprosecuted cases, we need to consider alternatives to prevent repeat harm or victimisation.

1.6 Report Structure in Detail

The Report is structured into 4 Parts:

PART A comprises 2 Sections providing an introduction to WMP, to fraud statistics headlines and to adapting or developing a public health approach to reduce the levels of fraud through prevention.

- Section 1: first provides brief details about the West Midlands Police and the headline fraud figures from Action Fraud;
- Section 2: a short summary of some of the themes towards adapting or developing a public health approach, taken from the *Volume II: the Background Report*.

PART B presents an analysis and interpretation of AF data in 3 Sections. The AF data is analysed by stated variables. This is then cross-referenced by postcode before being measured against current national data, AF data from 2014 and Disseminations data.

- Section 3: AF Data: Numbers of Cases, Losses and Victims by Fraud Category;
- Section 4: comparing data from Section 3 by postcode;
- Section 5: comparing AF data from Section 3 against contemporary national data, national AF data from 2014 and Disseminations data for comparison purposes.

PART C discusses in 2 Sections issues concerning the data and what the findings say about fraud in the WMP area and their basis for adapting or developing a public health approach.

- Section 6: issues relating to the quality and use of the data;
- Section 7: a summary of the findings by variables to present an evidence bases from which to discuss adapting or developing a public health approach response, including organisational shape and initial intervention initiatives.

PART D concludes the Report with 2 Sections that discuss any issues or constraints on adapting or developing a public health approach before assessing how far that approach may be developed within the context of the 4 Ps used by law enforcement to address certain crimes and then what initiatives may be proposed to explore the use of a public health approach to address the prevention of frauds.

- Section 8: constraints and perspectives on pursuing a public health approach;

[6] We are not discrediting victim and witness care programmes, both of which are important as shifts towards a victim-focussed rather than state-focussed justice system. But except when combined with learning how to avoid fraud, this 'support' is different from a fraud prevention focus.

[7] Although we are aware that all AF data is sent to police forces in case they wish to undertake their own sifting or intelligence analysis: this opportunity for independent sifting – and action following such sifting - is also resource-constrained.

- Section 9: how far a public health approach fits with the current use of the 4 Ps (Protect, Prevent, Pursue and Prepare) as a current law enforcement approach to certain crimes;
- Section 10: considers what initiatives may be undertaken to develop a public health approach, including ownership and trial interventions.

2. WHY CONSIDER A PUBLIC HEALTH APPROACH?

2.1 Introduction

In *Volume II: the Background Report,* we argued that the rise in fraud, the complexities of what is and is not a fraud (or a trading standards violation often given the more generic label 'scam'), and the low likelihood of victims receiving a positive response through the criminal justice process combine to lead any reasonable commentator to conclude that the current approach to fraud needs substantial reform. The value of developing a public health approach is that it focusses on harm reduction and prevention, with initiatives based on analysis of empirical data and aimed at specific groups or levels of intervention and the involvement of multiple organisations, rather than just the police.

The shift away from the police, with others taking primary responsibility for encouraging people to use, for example, the internet safely, reducing if not preventing levels of future frauds, and seeking to build up a sense of self-aware security and resilience, requires the organisation and coordination of both new and existing initiatives, and the engagement of a wider network of relevant organisations. Given how many frauds there are, and the current mechanisms for awareness and prevention, measures may need to be supplemented by developing a structured, coordinated and continuing outreach programme by trusted (and trustworthy) organisations and persons. It is tempting to cite well-known campaigns around seatbelts and smoking, but what is needed is a range of actions to combat a broad range of harms and evolving criminal techniques.

These might include public campaigns both to warn people about fraud dangers (as at present with 'Take Five') and to assist potential victims in becoming alert to and managing risks associated with financial activity through routine precautions; targeted experiments and 'mystery shopping' to emphasise the need to exercise basic due diligence about the uses of websites, for example, for younger people buying tickets for events; and personalised support offers for identified repeat victims or those whose mental and physical circumstances may plausibly make them especially vulnerable to/affected by fraud. Some of these are already being trialled by Trading Standards officers and perhaps others.

It is an approach already considered by the West Midlands Office of the Police and Crime Commissioner (WMOPCC). Focus groups from the WMOPCC's Fraud Summit in February 2020 proposed that: 'the ideal was seen to be a public health approach to tackling fraud; within the governance but also where investigators and victim support organisations work with GPs, social care, the third-party sector and other organisations in identifying economic abuse, and in providing interventions and specialist support. Activities that could be employed under such an approach include cross-agency campaigns, engagement strategies and training programmes.'

2.2 Limitations to Adapting or Developing the Approach

We emphasise that a UK public health approach should be a clearly-defined, resourced and organised transition from previous practice to an increasing emphasis – to paraphrase the NHS Long Term Plan - on the treatment and prevention of fraud by supporting individuals and organisations to adopt improved 'fraud healthy' behaviours with the objectives of (a) helping people to live safer, more secure lives, and (b) reducing the demand for (and possible delays in) treatment and care through the criminal justice system. We recognise that such an approach to fraud starts from a different point from that of medicine, in investment in research and perhaps in willingness to engage in randomisation of interventions and other features of the clinical trial environment.

Similarly, any focus on the three levels of intervention deployed within the health context - primary, secondary and tertiary prevention - may be blurred and imbalanced. We should not take for granted the willingness of organisations to engage, coordinate and/or accept that engagement will assist in preventing fraud or the fear of fraud when we consider, for example, GP interventions underpinned by commissioned mental health services. Victim Support has not been a strongly evidence-based crime prevention strategy hitherto, though caring for distressed people is a

Part A - Introduction

public good in itself. Victim support would require rigorous trial evidence of secondary or tertiary prevention of, say, anxiety or repeat victimisation to be considered a core part of any public health approach. Finally, we accept that public health approaches include interventions supported by evidence of effectiveness normally generated in rigorous randomised trials or quasi-experiments, though 'realist evaluations' of context-mechanism-outcome can be a more viable and valuable alternative.[8] Such experiments (and double-blind trials generally) involving not preventing frauds might be a challenge for research ethics committees and for public relations in business, policing and university sectors.

2.3 What this Report is Proposing

In recommending adapting for fraud a public health approach, we recognise that this is a case study in that the data relates to a single police area, that neither resources nor partnerships are yet in place and that in many ways, we are beginning the discourse on a public health approach to fraud rather than implementing it. Our recommendations are drawn from the empirical evidence as proposals rather than as an agreed programme. The recommendations also relate to potential interventions not yet supported by evidence of effectiveness generated through trials or pilot studies, as would be assumed within the public health context (and in many ways the recommendations will themselves propose what may be considered trials or pilot studies).

However, not to make recommendations on that basis is excessively cautious. We consider that the data in *Volume II: the Background Report* justifies this approach generally and certainly justifies the more detailed assessment of the primary data for the WMP Area, together with potential responses based on that assessment.

This is why we see this Report seeking ways of adapting or developing a public health approach in that it assesses the components noted in the College of Policing's approach – and in *Volume II: the Background Report* – that would:

- Take a public health approach to look at the epidemiology of frauds to understand who are the victims, why they may be victims, and are there any identifiable causes for their victimisation that can be distinguished from those present among non-victims and those less often victimised;
- Collect, collate and analyse empirical data to develop an evidence base to ensure that interventions are designed, delivered and tailored to be as effective as possible;
- Focus on prevention rather than on criminal justice interventions;
- Seek to promote partnership working, since the breadth of population need requires response (intervention) across many disciplines and services.

2.4 The Role of Data as the Platform from Which to Consider Public Health Approaches to Fraud

Drawing on a public health approach means seeking how to improve general health and safety[9] by looking for factors associated with victims that increase the likelihood that individual or groups may become a victim or a perpetrator of a crime. This involves shifting towards prevention, and a 'whole system' approach in developing responses.[10] The first step is the collection and analysis of available data to compile an evidence base from which to consider responses/interventions. Not all victims – especially not those who have lost nothing – consider they have been significantly harmed, but better information should be collated about those who consider that they been harmed and are seeking a response by reporting their case to AF in the first instance.

Every reputable study of crime data acknowledges the problem of attrition between victim/bystander identification as 'crime', the decision to report/not to report to the authorities, the recording of this as a crime, investigation and 'offenders brought to justice' (in UK Government terminology). The nature of this attrition process varies by offence, over time and between jurisdictions. Fraud is not the only offence where there is controversy over whether a reported crime is validly judged to be 'a crime' and recorded as such. But fraud has always been a special case, even before the Internet arrived. For both individuals and organisations, the opportunity cost of expected time spent reporting a fraud and expected benefits to self - and others – from doing so influences decisions to report or not, and except for some insurance cases, there

[8] Public Health England. 2021. *A brief introduction to realist evaluation*. London: Public Health England.
[9] Many medical interventions (including some Covid vaccinations) have negative health impacts on some people. So we cannot expect everyone to benefit or no-one to lose from a counter-fraud intervention either.
[10] Drawn from: Police Foundation. (2019). Public health approaches to crime prevention and the role of the police. London: Police Foundation/KPMG.

are few obvious material benefits (or loss avoidance or loss recovery) in reporting to the police rather than (for card and consumer banking frauds) merely to the financial institutions. Certainly, AF data tells us about those who felt angry or concerned enough about the threat or risk to their and/or others' financial well-being to report.

We therefore present some data about police-reported fraud in the West Midlands to assist the WMOPCC and others to consider both criminal justice and preventative options more clearly. AF data tell us about those frauds that have been identified as such (not always correctly) by those who have suffered actual or attempted loss and about which individual and organisational victims want something done and are prepared to go to the trouble of reporting to AF. (Though we note that AF data, while integrated by the ONS with data from the financial sector, are not integrated with reports to other public agencies such as Trading Standards, who also have a very large volume of fraud reports and a large dataset.)[11]

The basis for a public health approach is the aggregation and interpretation of empirical data and the evidence base to ensure that interventions are designed, delivered and tailored to be as effective as possible. We intend to analyse and assess fraud data relating to the WMP Area to see how far the data would allow us to make a more informed view of the added-value of such an approach and to make initial recommendations that:

- Looking behind an issue, problem or illness to understand who are more likely to be adversely affected;
- Focus on prevention;
- Propose initiatives that reflect levels of intervention;
- Propose partnerships and coordination as central, because the breadth of population need requires response (intervention) across many disciplines and services.

2.5 PART A SUMMARY

The West Midlands Police (WMP) is the second largest police force in the country; its fifth largest level of recorded crime is fraud while less than 1% of WMP's FTE serve in the Economic Crime Unit. Using the latest public Action Fraud (AF) data on referrals and outcomes for fraud and cybercrime broken down by Home Office police forces and other agencies in the UK for 1 April 2019 - 31 March 2020, 37,951 were referred to police forces, of which 6,363 resulted in a judicial outcome. 11.6% of AF reports go for investigation and only 16.7% of the referrals result in a judicial outcome – this is 2% of those reporting a fraud to AF, a very substantial attrition rate. From the research project's analysis of AF data relating to the WMP, the situation in West Midlands is little different from the country as a whole.

Notwithstanding the quite high probability that people will become victims of fraud – around 1 in 12 people annually (and far more over an average lifetime) - in the context of other demands on scarce policing resources such as dealing with violent crimes in the home and on the streets, fraud still occupies a subsidiary spot as a 'crime' problem in the minds of the public as well as in the minds and actions of the police. Coordinated preventive interventions with the general public and with victims will need to be considered very seriously, whether or not the resource for the fraud 'pursue' function is substantially increased to enhance detection and prosecutions. These interventions will need to be both primary (with those in the general population at risk of being defrauded) and secondary (to reduce repeat victimisation).

In such circumstances, and reflecting the conceptual thinking behind a public health approach, we proposed in *Volume II: the Background Report* that a public health approach could add value to fraud responses: but it would require a significant but essential shift to prevention. Given appropriate resources, the approach would require organisations other than just the police to take up primary responsibility for encouraging fraud awareness and applying this to situations where fraud is a risk, and to manage more actively lower expectations of any criminal justice engagement.[12]

[11] Even if integration occurred, there might be complexities in guaranteeing equivalent data protection standards. Trading standards data are available to police via PND, but we are informed that the process is laborious and may require some flexibility in terminology in search enquiries.

[12] Though evidence is lacking about current public expectations of criminal justice for frauds of different types.

Part A - Introduction

The point of a public health approach is to consider different intervention points and levels, involving awareness and self-driven prevention – including evidence from failed attempted frauds – as well as engagement with partners, businesses and others to reduce fraud through prevention. As with general and terrorist violence reduction, the public are unlikely to be aware of all interventions that reduce their risks, both before and after individuals or organisations become victims. Nevertheless, promotion and awareness of the wider picture is important to emphasise the holistic and community-wide nature of the approach. A sharper focus on identifying and helping people who are likely to become repeat victims is also important, both as a good practice in itself to reduce harm and to provide reassurance (if it does), and also to reduce actual levels of a range of frauds.

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

Presents an analysis and interpretation of AF data in 3 Sections. The AF data is analysed by a range of stated variables. This is then cross-referenced by postcode before being measured against current national data, AF data from 2014 and Disseminations data.

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

3. AF DATA: NUMBERS OF CASES, LOSSES AND VICTIMS BY FRAUD CATEGORY

3.1 Cases

The percent of all NFIB pre-defined fraud categories – see Annex 2 (Main WMP AF fraud categories; definitions) - in the WMP AF data for 4th May 2020 to 4th July 2021 are provided in Annex 3 (Period of WMP AF data). Out of the 50 fraud categories and over 20,000 recorded cases, most of the specified (49) categories of fraud yield very low levels of reported cases; only 5 categories have more than 5% of the total of reported cases – see - from the WMP AF data as follows:

• None of the Above (NFIB90):	27% of cases;
• Online Shopping and Auctions (NFIB3A)	24% of cases;
• Other Advance Fee Frauds (NFIB1H)	8% of cases;
• Other Consumer Non Investment Fraud (NFIB3D)	7% of cases;
• Cheque, Plastic Card and Online Bank Accounts	
• (not Payment Service Provider (PSP)[13] (NFIB5A)	7% of cases.

Of the remaining 45 categories, only 3 had more than 500 cases reported: NFIB2E (Other Financial Investment); NFIB3E (Computer Software Service Fraud); NFIB52C (Hacking - Social Media and Email). 27 categories had fewer than 100 cases and 15 had less than 10 cases each. The total reported losses associated with the 27 categories was over £16 million (or 8% of losses; with the removal of one case reported at over £14 million, the 27 categories involve over £2 million or 1% of reported losses).

3.2 Reported Losses

Of the 20,000+ reported cases, approximately two thirds of cases include a reported loss as stated by the victim. This totals over £227 million. Of the 5 main fraud categories by volume, the associated losses are:

None of the Above (NFIB90):	>£34 million;
Online Shopping and Auctions NFIB3A):	>£32 million;
Other Advance Fee Frauds (NFIB1H):	>£1 million;
Other Consumer Non Investment Fraud (NFIB3D):	> £6 million;
Cheque, Plastic Card and Online Bank Accounts (not PSP) (NFIB5A):	>£17 million.

7 other categories had similar losses, ranging from over £5 million to over £73 million but much smaller number of cases (under 2000 in total), reflecting not just the different natures of frauds but also the impetus for discovery and reporting: NFIB19 (Fraud by Abuse of Position of Trust); NFIB1D (Dating Scams); NFIB2A (Share Sales or Boiler Room Fraud): NFIB2B (Pyramid or Ponzi Schemes); NFIB2E (Other Financial Investment); NFIB52E (Hacking Extortion); NFIB8A (Corporate Employee Fraud).

The biggest reported loss - over £70 million - were associated with NFIB19 (Fraud by Abuse of Position of Trust). Three (NFIB51B: Denial of Service Attack Extortion; NFIB52D: Hacking - PBX/Dial Through; NFIB5C: Mortgage Related) have no recorded losses in the 7 reported cases, while 2 (NFIB51A: Denial of Service Attack and NFIB52A: Hacking – Server) report zero losses.

Of the 27 categories with fewer than 100 cases, the total reported losses were over £16 million (or 8% of losses; with the removal of one case reported at over £14 million, the 27 categories involve over £2 million in losses, equalling 1% of reported losses).

3.3 Mean and Median Losses

When considering the mean (average) loss by category, the picture changes slightly, emphasising the impact that a limited number of cases with high reported losses can have on the overall picture. Thus NFIB52E (Hacking Extortion), NFIB19 (Fraud by Abuse of Position of Trust), NFIB8A (Corporate Employee Fraud) and NFIB9 (Business Trading Fraud) had mean losses in excess of £100,000. In NFIB52E (Hacking extortion), one case claims a loss of £10 million, although the narrative of the case suggests that the complainant worked for a firm whose software was hacked and the sum could have been paid to release the data while the report appears to have been made because of the risk from the hackers' potential access to the personal and financial details of the person reporting who may not have directly personally suffered a loss at the time of reporting).

For this reason, we have generally opted for displaying the median losses, since outlier losses have a disproportionate effect on averages (though

[13] PSP is a payment service provider, for example PayPal and World Pay, that is not a bank, dealing in electronic money transfers.

Part B - The Data: Reports of fraud for the WMP area for May 2020 to July 2021

these large losses may be important as a trigger for crime investigation and loss reduction, and sometimes but not always as an indicator of social harm). Here the value per case is significantly lower and the categories vary. Thus, the main categories for median losses over £5000 are: NFIB10 (False Accounting); NFIB14 (Fraudulent Applications for Grants from Government Funded Organisations); NFIB9 (Business Trading Fraud); NFIB8B (Corporate Procurement Fraud); NFIB8A (Corporate Employee Fraud); NFIB16B (Pension Fraud committed on Pensions); NFIB4B (Fraudulent Applications for Grants from Charities).

We stress that all these frauds were considered by their victims to be important enough to take the trouble to report to AF, but we note that the five fraud category types – NFIB1H, NFIB3A, NFIB3D, NFIB90 and NFIB 5A - with the greatest volume of reported cases reflect significantly lower median losses, ranging between £30 and £500 median loss per case. Thus, in terms of cases by volume, the five largest categories do not figure significantly in terms of median (or mean) reported losses. (And nor are they reflected among the majority of cases disseminated to WMP by NFIB, nor of the cases that are selected for dissemination to police forces by NFIB.)[14]

3.4 Which Category – Individual or Organisation - is Most at Risk?

Approximately 94% of reported cases came from individuals and 6% from organisations. Organisational victims appear to be at lowest risk both in terms of volume of reported cases and the range across the NFIB categories, though in addition to non-reporting issues which we have not investigated here, this data needs to be normalised against the number of firms. To illustrate the divergence between the risk facing individuals and organisations, and why fraud is not a uniform phenomenon, we note in table 5 those categories where the individual is at significantly less risk of fraud and where organisations are at a much greater risk of fraud. In the case of the higher levels of organisational risk, the number of cases is very low for each category (less than 1% of all cases); see Table 3.

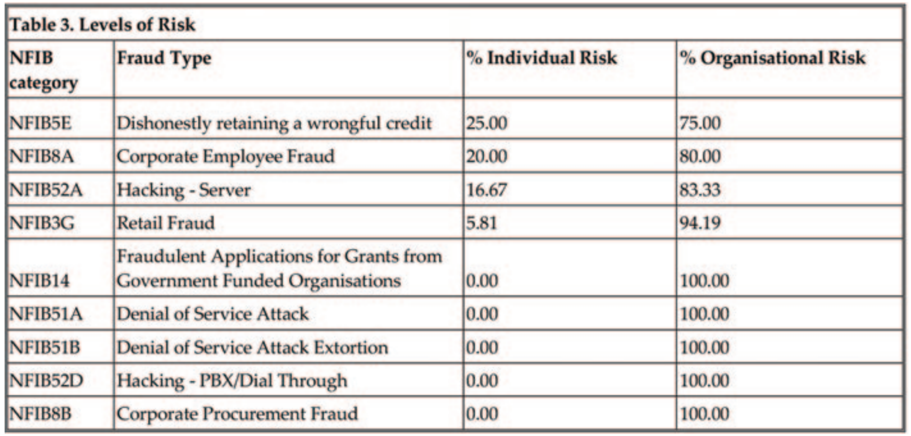


Table 3. Levels of Risk

NFIB category	Fraud Type	% Individual Risk	% Organisational Risk
NFIB5E	Dishonestly retaining a wrongful credit	25.00	75.00
NFIB8A	Corporate Employee Fraud	20.00	80.00
NFIB52A	Hacking - Server	16.67	83.33
NFIB3G	Retail Fraud	5.81	94.19
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	0.00	100.00
NFIB51A	Denial of Service Attack	0.00	100.00
NFIB51B	Denial of Service Attack Extortion	0.00	100.00
NFIB52D	Hacking - PBX/Dial Through	0.00	100.00
NFIB8B	Corporate Procurement Fraud	0.00	100.00

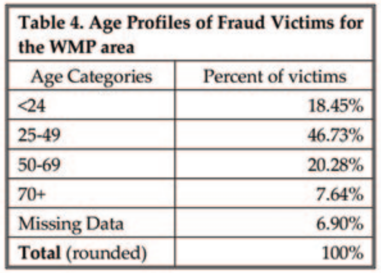


Table 4. Age Profiles of Fraud Victims for the WMP area

Age Categories	Percent of victims
<24	18.45%
25-49	46.73%
50-69	20.28%
70+	7.64%
Missing Data	6.90%
Total (rounded)	100%

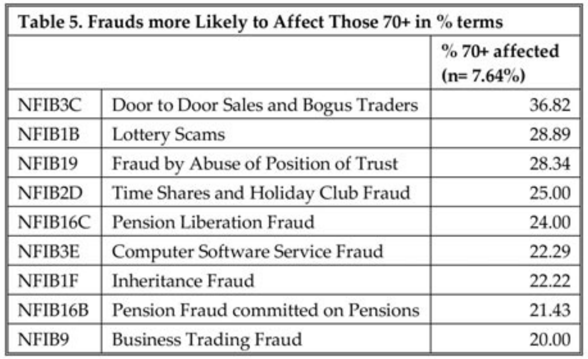


Table 5. Frauds more Likely to Affect Those 70+ in % terms

		% 70+ affected (n= 7.64%)
NFIB3C	Door to Door Sales and Bogus Traders	36.82
NFIB1B	Lottery Scams	28.89
NFIB19	Fraud by Abuse of Position of Trust	28.34
NFIB2D	Time Shares and Holiday Club Fraud	25.00
NFIB16C	Pension Liberation Fraud	24.00
NFIB3E	Computer Software Service Fraud	22.29
NFIB1F	Inheritance Fraud	22.22
NFIB16B	Pension Fraud committed on Pensions	21.43
NFIB9	Business Trading Fraud	20.00

3.5 Age Variations

The age profile for the WMP area is presented in Table 4. The likelihood of becoming a victim of fraud varies across the categories (see Figure 1), but almost two thirds of reporting victims are under 50, though this has not been normalised for the region's population (the median UK age is 40.) In accordance with what one would expect from routine activities models, 70% of pension frauds concern those over 50, and two-thirds of victims in inheritance frauds are under 50.

Some types of frauds are more prevalent among different age groups – nearly half of lender loan (advance fee) frauds are against the 25-49 age group - while others, such as lottery scams, show an equal distribution among the 25-49, 50-69 and over 70 groups. Dating scams, like online

[14] By way of comparison, in the year to March 2022, the median cost of fraud against individuals in England and Wales was £79; it was £95 for bank and credit account fraud; £53 for consumer and retail fraud; and £100 for advance fee fraud: see *Nature of crime: fraud and computer misuse year ending March 2022*, ONS

shopping and auction frauds, are more closely associated with those between 25 and 69. However this is a very large age range, so it might be clearer to note that people aged 70 and over appear to be relatively less vulnerable to dating scams than the stereotypes would suggest. Similarly, those over 70 do not appear to be vulnerable to all types of financial frauds: those over 70 are more likely to be victims of pension scams, but less likely to be victims of NFIB2B (Pyramid or Ponzi schemes). Table 5 illustrates those categories where those over 70 are disproportionally represented in the age distribution profile. The most significant in terms of number of cases are NFIB3E, NFIB19 and NFIB3C.

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

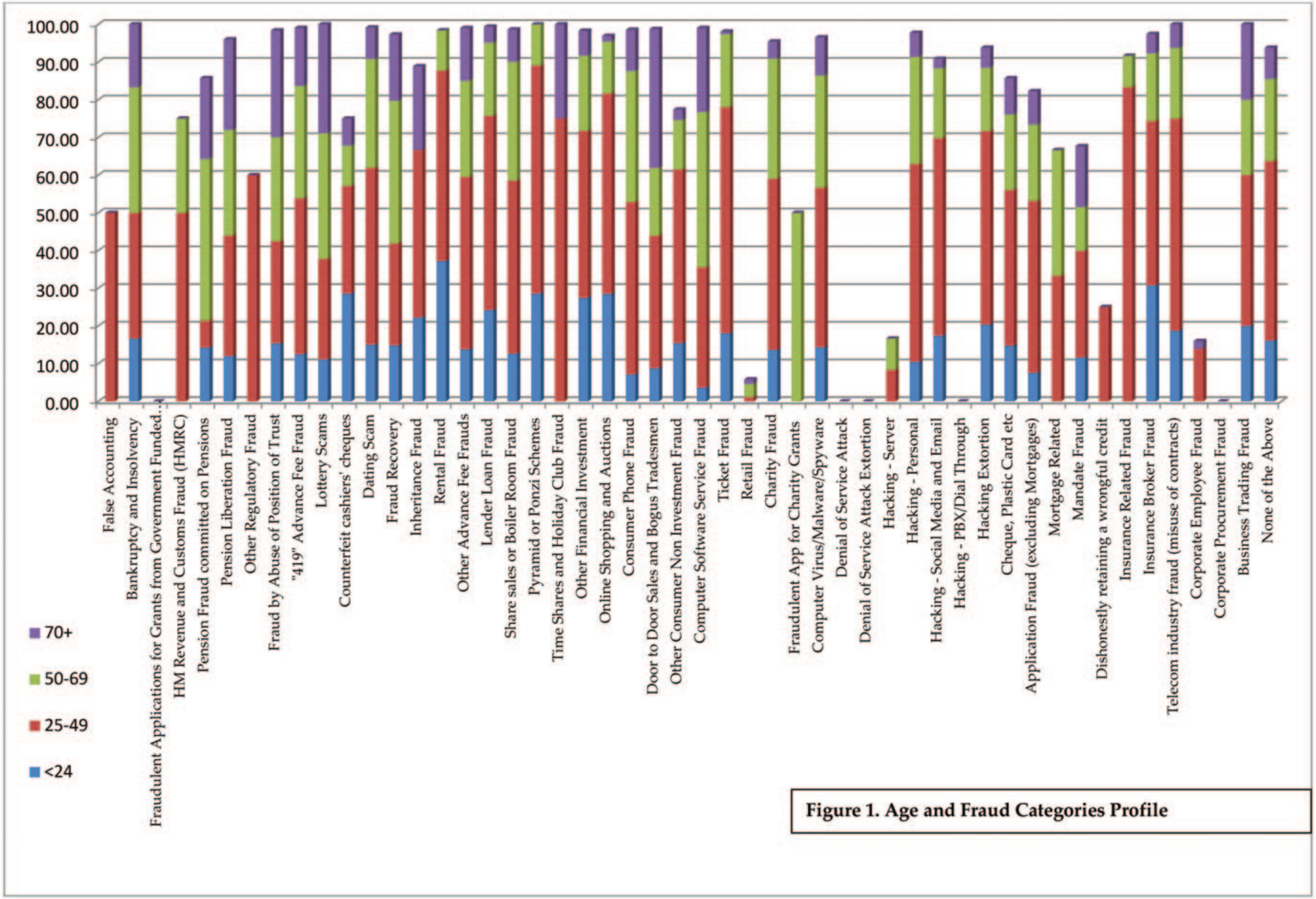


Figure 1. Age and Fraud Categories Profile

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

It is also possible to develop a picture of relative risk – those frauds to which particular age groups are more likely to be susceptible: see Table 6.

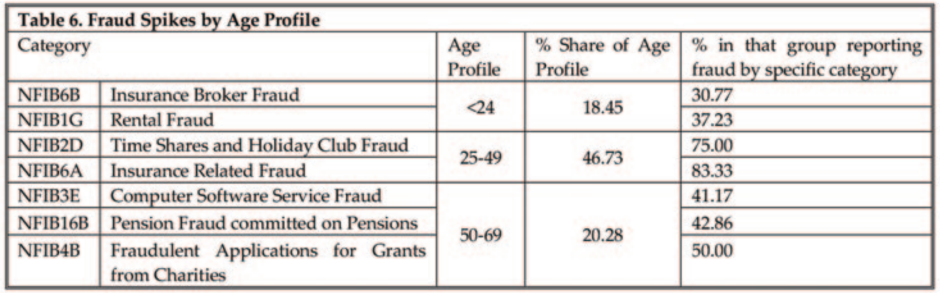


Table 6. Fraud Spikes by Age Profile

Category		Age Profile	% Share of Age Profile	% in that group reporting fraud by specific category
NFIB6B	Insurance Broker Fraud	<24	18.45	30.77
NFIB1G	Rental Fraud			37.23
NFIB2D	Time Shares and Holiday Club Fraud	25-49	46.73	75.00
NFIB6A	Insurance Related Fraud			83.33
NFIB3E	Computer Software Service Fraud	50-69	20.28	41.17
NFIB16B	Pension Fraud committed on Pensions			42.86
NFIB4B	Fraudulent Applications for Grants from Charities			50.00

3.6 Ethnicity Variations

We can undertake a similar exercise by ethnicity (as categorised by AF), although there is much missing data for this component, which has generated difficulties in the initial analysis. However, looking at whether ethnicity is correlated with susceptibility to particular types of fraud, we note that NFIB6B (Insurance Broker Fraud), NFIB2E (Other Financial Investment)[15] and NFIB3F (Ticket Fraud) are more likely to be more strongly associated with being Asian or British Asian; NFIB2B (Pyramid or Ponzi Schemes) with being Black or Black British; NFIB1F (Inheritance Fraud) with being Mixed, NFIB16B (Pension Fraud committed on Pensions) with Other, NFIB3E (Computer Software Service Fraud) with being White and NFIIB4A (Charity Fraud) with being White Other. However, the small number of cases for some fraud types should make us cautious about inferring that these ethnicities are at a significantly higher risk, still less that they are targeted because of their ethnicity, and this study has not had the chance to explore these ethnic variations more deeply.

3.7 Vulnerability Variations

Vulnerability is an important construct, and the source of much confusion between different enforcement and safeguarding agencies, e.g., between those that statistically are of higher risk and those on whom there is special impact/harm if and when victimised. In terms of reducing the harms done to 'vulnerable victims', the WMP AF data suggests that around 42% of those reporting fraud have been fraud victims before, so this is a substantial category (see Table 7 for all categories where 50% or more of fraud victims are repeat victims of fraud). Of these, we wanted to know whether repeat victimisation differs by fraud category. There were statistically significant differences, e.g., over a third of online shopping and auctions (NFIB3A) victims were repeat victims. Disregarding missing data and the ethnic distribution of the population in the WMP area, 45% of online shopping fraud victims were white, compared to 27% Asian and 10% Black or White Other - and in line with the percent of population composition of the dataset. Again, we emphasise that this is a figure for those who have been victims previously: it does not tell us what the risks of future repeat victimisation are for those victimised the first time.

[15] NFIB2E is dealt with under the Fraud Act 2006 Section 2 ("…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss)". The NFIB category guidance notes:

the word "investment" is used in connection with a wide range of schemes offering income, interest or profit in return for a financial investment. "Investment" is often used loosely, and sometimes misleadingly, in order to disguise the true nature of a fraud; e.g. pyramid schemes, chain letters or other types of scheme where a return depends on persuading others to join. The term "investment" is commonly used in connection with the purchase of something - such as high value or rare goods, stocks and shares, property - in the expectation that what is purchased will increase in value, and even provide an exceptional return compared to other forms of investment. It is not always understood by potential investors that there is a wide range of so-called investments which are unregulated.

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

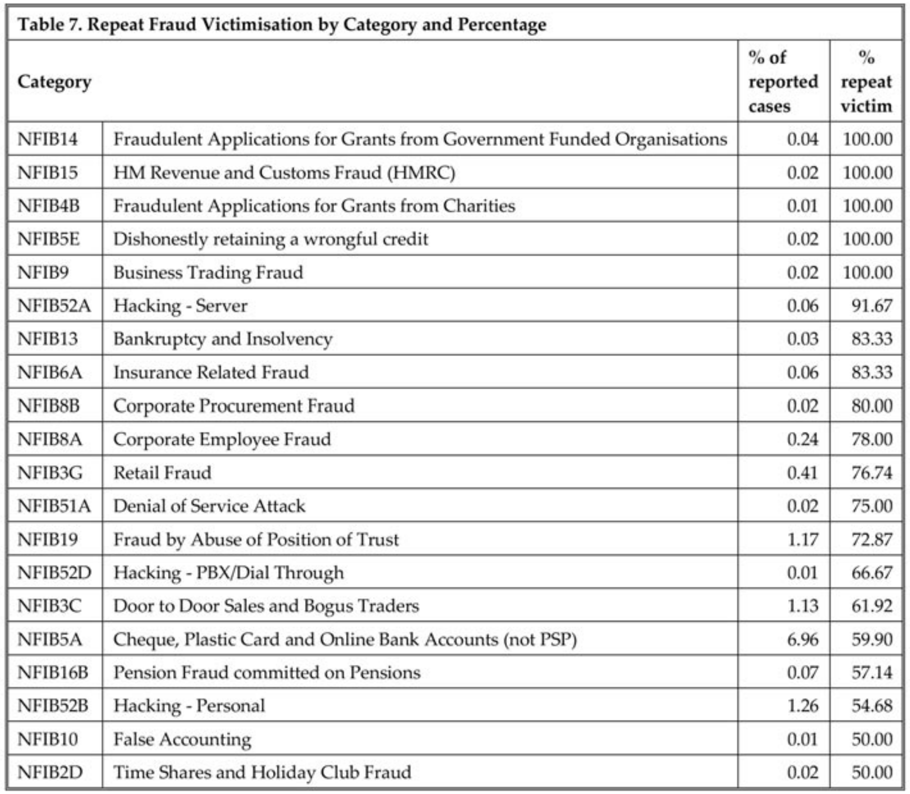


Table 7. Repeat Fraud Victimisation by Category and Percentage

Category		% of reported cases	% repeat victim
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	0.04	100.00
NFIB15	HM Revenue and Customs Fraud (HMRC)	0.02	100.00
NFIB4B	Fraudulent Applications for Grants from Charities	0.01	100.00
NFIB5E	Dishonestly retaining a wrongful credit	0.02	100.00
NFIB9	Business Trading Fraud	0.02	100.00
NFIB52A	Hacking - Server	0.06	91.67
NFIB13	Bankruptcy and Insolvency	0.03	83.33
NFIB6A	Insurance Related Fraud	0.06	83.33
NFIB8B	Corporate Procurement Fraud	0.02	80.00
NFIB8A	Corporate Employee Fraud	0.24	78.00
NFIB3G	Retail Fraud	0.41	76.74
NFIB51A	Denial of Service Attack	0.02	75.00
NFIB19	Fraud by Abuse of Position of Trust	1.17	72.87
NFIB52D	Hacking - PBX/Dial Through	0.01	66.67
NFIB3C	Door to Door Sales and Bogus Traders	1.13	61.92
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96	59.90
NFIB16B	Pension Fraud committed on Pensions	0.07	57.14
NFIB52B	Hacking - Personal	1.26	54.68
NFIB10	False Accounting	0.01	50.00
NFIB2D	Time Shares and Holiday Club Fraud	0.02	50.00

Cases involving a large number of victims are Cheque, Plastic Card and Online Bank Accounts (not PSP) fraud, Fraud by Abuse of Position of Trust, Hacking (Personal) and Door to Door Sales and Bogus Traders. When matched with the two higher levels of victim vulnerability, the most likely fraud categories for large numbers of vulnerable repeat victims are: Hacking (Personal), Time Shares and Holiday Club Fraud, Other Financial Investment, Dating Scams, and Hacking (Extortion).

We should separate organisational and individual victims (though some SMEs straddle both categories): it is less surprising that high rates of repeat victimisation of employee fraud, retail fraud and fraud by abuse of position of trust occur against corporate victims, since these are businesses that can readily be targeted by employees, managers/directors and outsiders, alone or in collusion. What we are unable to clarify from the data is whether 'repeat' applies to the same type of offence, to a range of categories, to the frequency and rapidity of the victimisation, or to multiple frauds within the same scam (such as escalating payments in a NFIB1A [Advanced Fee] fraud). This would be a fruitful issue to be explored by the changes to Action Fraud that are currently under way.

3.8 Postcode Variations

In order to determine whether the potential interventions are a uniform force-wide issue or whether there are identifiable variations by the 5 postcodes (B=Birmingham; CV=Coventry; DY=Dudley; WS=Walsall and WV=Wolverhampton), the research has reviewed the data against the findings in the previous Sections.

There are age and ethnicity variations across the postcodes by volume. In general terms the age profiles against number of cases changes little across postcodes: however, in CV, those under 24 are slightly more likely to be victims of fraud, while in DY and WV, those aged between 50-59 are also more likely to be at risk of becoming a victim of fraud. There are some minor ethnic variations in the proportions of victims per area: Asian victims are much lower in DY than the WMP area average, while White victims are more common in both DY and WS.

The distribution across the 5 main fraud categories by volume between postcodes show similar percentages, although at least one postcode appears to have more cases of fraud than the other postcodes per head of population. Overall, the number of cases of reported fraud is less than 1% of the population

More generally, the volume of cases in proportion to the distribution of the population is quite consistent across postcodes, although with slight variations by postcode within the main 5 categories as follows:

- For Coventry (CV) these are: NFIB52C (Hacking - Social Media and Email) and NFIB2E (Other Financial Investment);
- For Dudley (DY) these are: NFIB2E (Other Financial Investment) and NFIB3D (Other Consumer Non Investment Fraud);
- For Walsall (WS) this is: NFIB5A (Cheque, Plastic Card and Online Bank

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

Accounts (not PSP))

- For Wolverhampton this is: NFIB3D (Other Consumer Non Investment Fraud).

Two postcodes have additional categories with noticeable but not statistically significant variations in numbers of cases as follows:

- For Coventry this is: NFIB1D (Dating Scams);
- For Dudley these are: NFIB1D (Dating Scams) and NFIB50A (Computer Virus/Malware/Spyware).

In terms of the distribution of losses, the B postcode had nearly 60% of all cases, accounting for 77% of the reported losses (over £171 million). CV accounted for 13% of the cases and 4% of the losses; DY accounted for 8% of the cases and 4% of the losses; WS accounted for 8% of the cases and 11% of the losses; and WV accounted for 11% of the cases and 3% of the losses. The WS data accounts for 59% of the reported losses under NFIB5A [Cheque, Plastic Card and Online Bank Accounts (not PSP)] and 71% of reported losses under NFIB8A [Corporate Employee Fraud].

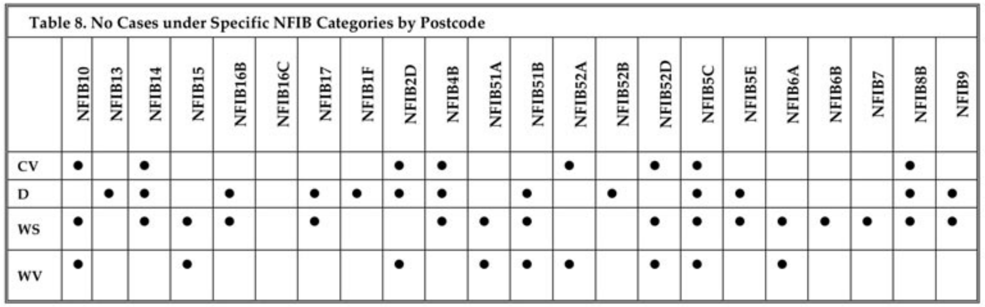


Table 8. No Cases under Specific NFIB Categories by Postcode

	NFIB10	NFIB13	NFIB14	NFIB15	NFIB16B	NFIB16C	NFIB17	NFIB1F	NFIB2D	NFIB4B	NFIB51A	NFIB51B	NFIB52A	NFIB52B	NFIB52D	NFIB5C	NFIB5E	NFIB6A	NFIB6B	NFIB7	NFIB8B	NFIB9
CV	●		●						●	●			●		●	●					●	
D		●	●		●		●	●	●	●		●		●		●	●				●	●
WS	●		●	●	●		●			●	●	●			●	●	●	●	●	●	●	●
WV	●			●					●		●	●	●		●	●		●				

Overall, there are slight variations in terms of the main types of reported frauds to AF by volume. While the B postcode contains reported frauds across all 50 categories, some postcodes have no cases in some fraud categories: see Table 8.

Average or mean losses will clearly influence distribution by postcode if the number of cases is small. The profile suggests that there are variations across postcodes and that the fraud mean loss profile is not entirely consistent across the WMP area when distributed by postcode, apart from Birmingham where the mean losses were higher the overall WMP average loss/case figure in 3 categories (NFIB2E [Hacking Extortion], NFIB19 [Fraud by Abuse of Position of Trust], and NFIB9 [Business Trading Fraud]). The 5 high losses vary across postcodes, and are of relatively low value, apart from NFIB5D (Mandate Fraud) and NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)) in Walsall and NFIB3C (Door to Door Sales and Bogus Traders) in Birmingham. Apart from Wolverhampton, all the other four categories suffer significant mean losses from NFIB8A (Corporate Employee Fraud).

It is more illuminating to look at postcode variations using median losses. In terms of the 5 categories with the largest number of reported cases - NFIB90, NFIB3A, NFIB1H, NFIB3D and NFIB5A – these have fairly consistently low medians (usually below £500); these are generally replicated across postcodes. In terms of median losses by fraud category over £1000 some categories show similar losses across postcodes: these include Fraud Recovery (NFIB1E), Fraud by Abuse of Position of Trust (NFIB19), Counterfeit cashiers' cheques (NFIB1C) and Dating Scams (NFIB1D). Others are more post-code-specific.

Thus, both CV and WV postcodes, and to a lesser extent postcode WS, suffer a broad range of financial frauds: "419" Advance Fee Fraud (NFIB1A), Lottery Scams (NFIB1B), Inheritance Fraud (NFIB1F), Rental Fraud (NFIB1G), Other Advance Fee Frauds (NFIB1H) and Lender Loan Fraud (NFIB1J). Unusually, and outside the B postcode, one postcode – DY – appears to be subject to frauds less common elsewhere: False Accounting (NFIB10); Corporate Employee Fraud (NFIB8A); Mandate Fraud (NFIB5D); Other Financial Investment (NFIB2E); Insurance Broker Fraud (NFIB6B) and Ticket Fraud (NFIB3F). It is not clear to us why that should be the case.

Part B - The Data: Reports of fraud for the WMP area for May 2020 to July 2021

4. COMPARING NUMBERS OF CASES, LOSSES AND VICTIMS BY POSTCODE

4.1 Comparisons by Districts and the WMP Area: Age and Ethnicity Variations

The age-fraud relationship is relatively similar across the postcodes. However, some fraud categories were more prominent in some areas; for example, in B, over 70% of pension liberation frauds affected the 25-69 group while, in DY, 60% of those 70+ were affected. Where some ethnic groups appear to be disproportionately likely to be fraud victims, taking into account their numbers in the population, it is possible in terms of planning area- or group-specific prevention messaging - to correlate these numbers with postcode distribution to provide a geographic focus to any initiative.

Thus Table 9 provides a first attempt to map specific fraud categories across postcodes by ethnicity.

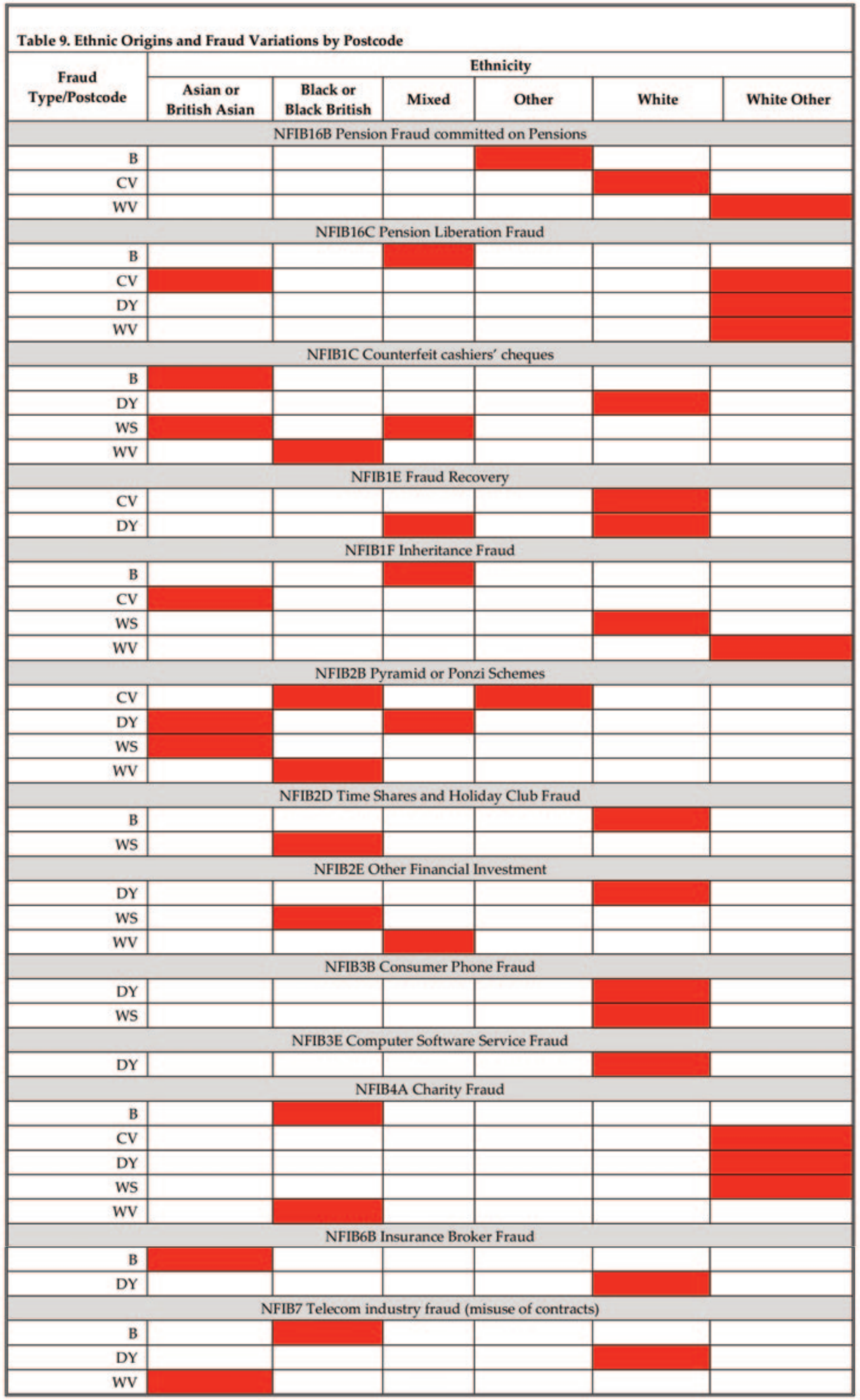


Table 9. Ethnic Origins and Fraud Variations by Postcode

Fraud Type/Postcode	Ethnicity					
	Asian or British Asian	Black or Black British	Mixed	Other	White	White Other
NFIB16B Pension Fraud committed on Pensions						
B				🟥		
CV					🟥	
WV						🟥
NFIB16C Pension Liberation Fraud						
B			🟥			
CV	🟥					🟥
DY						🟥
WV						🟥
NFIB1C Counterfeit cashiers' cheques						
B	🟥					
DY					🟥	
WS	🟥		🟥			
WV		🟥				
NFIB1E Fraud Recovery						
CV					🟥	
DY			🟥		🟥	
NFIB1F Inheritance Fraud						
B			🟥			
CV	🟥					
WS					🟥	
WV						🟥
NFIB2B Pyramid or Ponzi Schemes						
CV		🟥		🟥		
DY	🟥		🟥			
WS	🟥					
WV		🟥				
NFIB2D Time Shares and Holiday Club Fraud						
B					🟥	
WS		🟥				
NFIB2E Other Financial Investment						
DY					🟥	
WS		🟥				
WV			🟥			
NFIB3B Consumer Phone Fraud						
DY					🟥	
WS					🟥	
NFIB3E Computer Software Service Fraud						
DY					🟥	
NFIB4A Charity Fraud						
B		🟥				
CV						🟥
DY						🟥
WS						🟥
WV		🟥				
NFIB6B Insurance Broker Fraud						
B	🟥					
DY					🟥	
NFIB7 Telecom industry fraud (misuse of contracts)						
B		🟥				
DY					🟥	
WV	🟥					

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

The data suggests some ethnic groups may be more susceptible to certain types of fraud. These include White/White Other groups for pension frauds; or Asian, British Asian, Black, Black British and Mixed Groups for Ponzi schemes. However, this differential susceptibility hypothesis requires further exploration to understand any underlying patterns of opportunity and vulnerability.

4.2 Comparisons by Districts and the WMP Area: Vulnerability Variations

The data showed overall similar rates of repeat victimisation within postcode areas averaging around 41%, though Dudley (37%) was slightly lower. We have not statistically controlled for this, but given differential populations in those urban areas, of those repeat victims, 61% are in Birmingham, 12% in Coventry, 11% in Wolverhampton, 8% in Dudley, and 8% in Walsall. Table 10 notes that a majority of fraud categories have 50%+ repeat victims across postcodes, with four fraud categories – NFIB19 (Fraud by Abuse of Position), NFIB3G (Retail Fraud), NFIB3C (Door to Door Sales and Bogus Traders), NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)), and NFIB8A (Corporate Employee Fraud) – indicating high levels of repeat victimisation across all postcodes (highlighted in blue. Others such as NFIB 13 (Bankruptcy and Insolvency), NFIB15 (HM Revenue and Customs Fraud (HMRC)), NFIB52A (Hacking – Server), NFIB5E (Dishonestly retaining a wrongful credit) and NFIB9 (Business Trading Fraud), show a very high level of repeat victimisation across several postcodes.

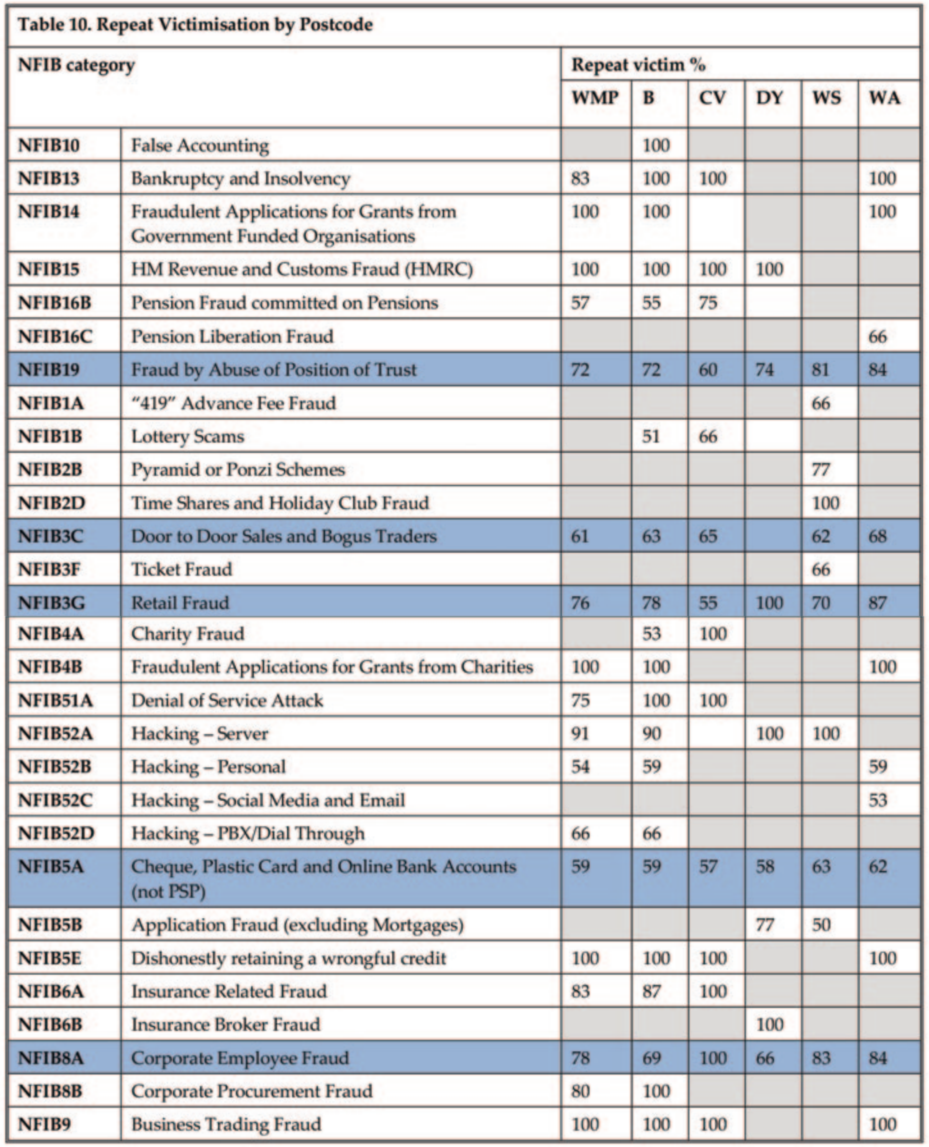


Table 10. Repeat Victimisation by Postcode

NFIB category		Repeat victim %					
		WMP	B	CV	DY	WS	WA
NFIB10	False Accounting		100				
NFIB13	Bankruptcy and Insolvency	83	100	100			100
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	100	100				100
NFIB15	HM Revenue and Customs Fraud (HMRC)	100	100	100	100		
NFIB16B	Pension Fraud committed on Pensions	57	55	75			
NFIB16C	Pension Liberation Fraud						66
NFIB19	Fraud by Abuse of Position of Trust	72	72	60	74	81	84
NFIB1A	"419" Advance Fee Fraud					66	
NFIB1B	Lottery Scams		51	66			
NFIB2B	Pyramid or Ponzi Schemes					77	
NFIB2D	Time Shares and Holiday Club Fraud					100	
NFIB3C	Door to Door Sales and Bogus Traders	61	63	65		62	68
NFIB3F	Ticket Fraud					66	
NFIB3G	Retail Fraud	76	78	55	100	70	87
NFIB4A	Charity Fraud		53	100			
NFIB4B	Fraudulent Applications for Grants from Charities	100	100				100
NFIB51A	Denial of Service Attack	75	100	100			
NFIB52A	Hacking – Server	91	90		100	100	
NFIB52B	Hacking – Personal	54	59				59
NFIB52C	Hacking – Social Media and Email						53
NFIB52D	Hacking – PBX/Dial Through	66	66				
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	59	59	57	58	63	62
NFIB5B	Application Fraud (excluding Mortgages)				77	50	
NFIB5E	Dishonestly retaining a wrongful credit	100	100	100			100
NFIB6A	Insurance Related Fraud	83	87	100			
NFIB6B	Insurance Broker Fraud				100		
NFIB8A	Corporate Employee Fraud	78	69	100	66	83	84
NFIB8B	Corporate Procurement Fraud	80	100				
NFIB9	Business Trading Fraud	100	100	100			100

Part B - The Data: Reports of fraud for the WMP area for May 2020 to July 2021

5. COMPARISON OF AF DATA AGAINST CONTEMPORARY NATIONAL DATA, HISTORICAL DATA AND DISSEMINATIONS DATA

5.1 How Does the AF Fraud Profile Map against National Data?

The WMP AF data for the volume of cases are similar to the national picture provided by AF (though the latter covers the slightly different period from November 2020 to November 2021). Of just over 487,000 reports nationally, the most reported categories are listed in Table 11.

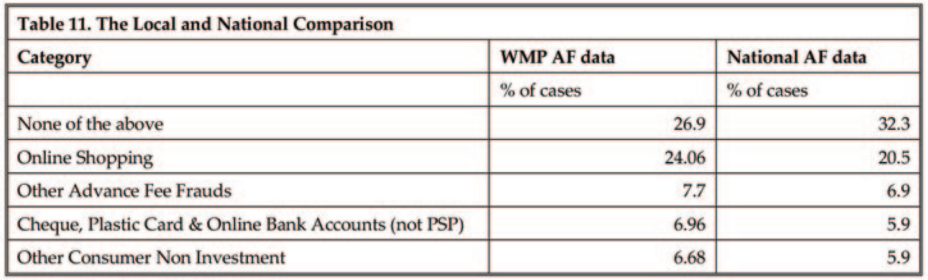


Table 11. The Local and National Comparison

Category	WMP AF data	National AF data
	% of cases	% of cases
None of the above	26.9	32.3
Online Shopping	24.06	20.5
Other Advance Fee Frauds	7.7	6.9
Cheque, Plastic Card & Online Bank Accounts (not PSP)	6.96	5.9
Other Consumer Non Investment	6.68	5.9

5.3 How Does the WMP AF Fraud Profile Map against Historical Data?

Total reports to AF have risen over the years (from nearly 73,000 in the year to March 2009 to over 200,000 in the year to March 2014 when our first snapshot analysis of AF data took place). Contemporary data shows that the overall reported fraud landscape has not changed significantly since 2014[16] - see Annex 5 (A Time Comparison: 2014 and 2020-21). Within categories, there are some noticeable changes. Cases involving NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)) and NFIB5B (Application Fraud (excluding Mortgages)) have dropped. On the other hand, investments scams, such as Boiler room frauds and Ponzi schemes, have increased. As WM people use the web more, online shopping and dating scams have risen, though these tend not to generate big increases in cases: see Table 12. The fall in computer software service fraud is likely to be a temporary artefact of the closure of some overseas call centres during parts of the pandemic. Our AF dataset does not enable us to separate such cases out, but internal TSB and other bank data reveal the dramatic growth in investment frauds via social media.[17] Indeed, banks' own individual or collective analysis of customer fraud data are a fruitful avenue for future insights and prevention efforts.

In terms of national data, albeit difficult to make accurate comparison at specific points in time, the rise in the number of reported cases for the 5 main fraud categories is noticeable. Variations in median loss over time also show some interesting insights into changes in median losses between the national 2014 data and the WMP AF data for 2020-21. In the financial services and financial regulation areas (including pensions), median losses to individuals have dropped, while the business and organisational sectors have seen significant rises.

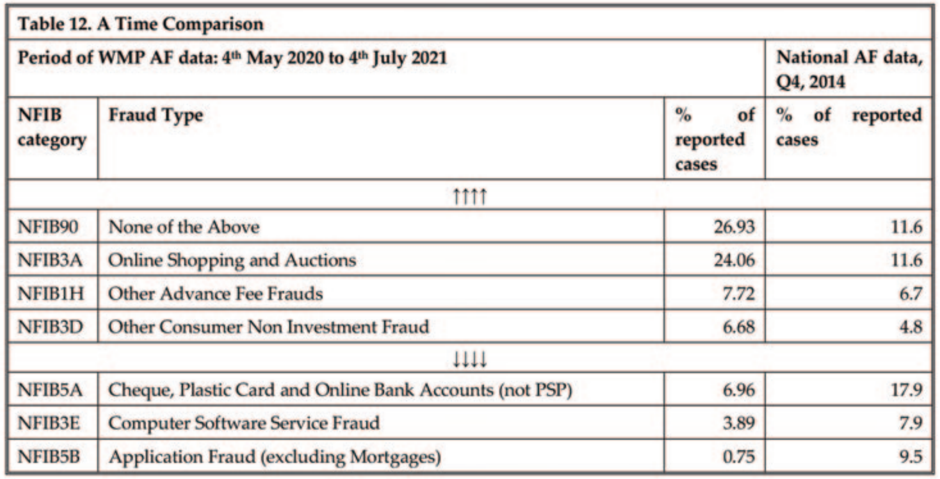


Table 12. A Time Comparison

Period of WMP AF data: 4th May 2020 to 4th July 2021			National AF data, Q4, 2014
NFIB category	Fraud Type	% of reported cases	% of reported cases
↑↑↑↑			
NFIB90	None of the Above	26.93	11.6
NFIB3A	Online Shopping and Auctions	24.06	11.6
NFIB1H	Other Advance Fee Frauds	7.72	6.7
NFIB3D	Other Consumer Non Investment Fraud	6.68	4.8
↓↓↓↓			
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96	17.9
NFIB3E	Computer Software Service Fraud	3.89	7.9
NFIB5B	Application Fraud (excluding Mortgages)	0.75	9.5

[16] See Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. 2015. The Implications of Economic Cybercrime for Policing. Research report: Technical Annex, City of London Corporation. City of London Corporation.

[17] https://www.thetimes.co.uk/article/facebook-and-instagram-blamed-for-surge-in-scams-jqtn9sdsm.

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

The biggest median loss changes for losses over £5000 for the two periods show significant increases associated with: NFIB10 (False Accounting); NFIB8A (Corporate Employee Fraud); NFIB8B (Corporate Procurement Fraud); NFIB14 (Fraudulent Applications for Grants from Government Funded Organisations). On the other hand, many more categories show a significant decrease in median losses; see Table 14 (for illustrative purposes, since the datasets cover different lengths of time). For the five largest reported cases by volume, the median money and real (inflation-adjusted) value of all except cheque/card/online banking (NFIB5A) has fallen since 2014, and continues to be relatively modest amounts lost, if one disregards the income/wealth of victims.

5.3 Disseminations Data

5.3.1 Distribution

Between 1st April 2020 and 31st March 2021, the NFIB disseminated just over 1200 reports for investigation; 14% of these were transferred from other forces via NFIB for dissemination to the WMP, because they were regarded by them as more appropriate for the WMP. In the case of 14 NFIB categories, it would appear that no cases were disseminated in that particular period of time, including:

NFIB13	Bankruptcy and Insolvency
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations
NFIB15	HM Revenue and Customs Fraud
NFIB16B	Pension Fraud committed on Pensions
NFIB16C	Pension Liberation Fraud
NFIB17	Other Regulatory Fraud
NFIB2D	Time Shares and Holiday Club Fraud
NFIB3B	Consumer Phone Fraud
NFIB3F	Ticket Fraud
NFIB3G	Retail Fraud
NFIB4A	Charity Fraud
NFIB4B	Fraudulent Applications for Grants from Charities
NFIB51A	Denial of Service Attack
NFIB51B	Denial of Service Attack Extortion

Of the remaining categories that were disseminated, the greatest number – reflecting more than 5% of the total number of disseminated cases – were: NFIB19 (Fraud by Abuse of Position of Trust) – 15.6%; NFIB2E (Other Financial Investment) – 10.9%; NFIB3A (Online Shopping and Auctions) – 12.6%; NFIB52C (Hacking – Social Media and Email) – 8.3%; NFIB5A (Cheque, Plastic Card and Online Bank Accounts [not PSP]) – 7% of cases; NFIB90 (None of the Above) – 7% of cases.

5.3.2 Composition and Outcomes

Of the disseminated cases, over 80% had been or were still classified as 'under investigation' for more than 12 months, which may reflect low investigative resources as well as the inherent difficulty of pursuit in fraud cases. In terms of outcomes, a small number were transferred to another agency and about 80% were discontinued for a variety of reasons; the largest number concerned the Outcome 15 reporting category where evidential difficulties prevent further action. This includes but is not restricted to cases where the suspect has been identified, the victim supports action, the suspect has been circulated as wanted but cannot be traced and nothing more can be done in relation to arrest.

In terms of judicial or other outcomes, 3% were charged or summoned; nearly 2% were cautioned; a handful were subject to community resolution or other guidance. In short, around 10% of reported fraud is likely to be triaged and disseminated. Of the disseminated cases, less than 5% will result in some form of positive outcome. Overall, as noted earlier, less than 1% of all reported fraud is likely to end up being subject to a police investigation.

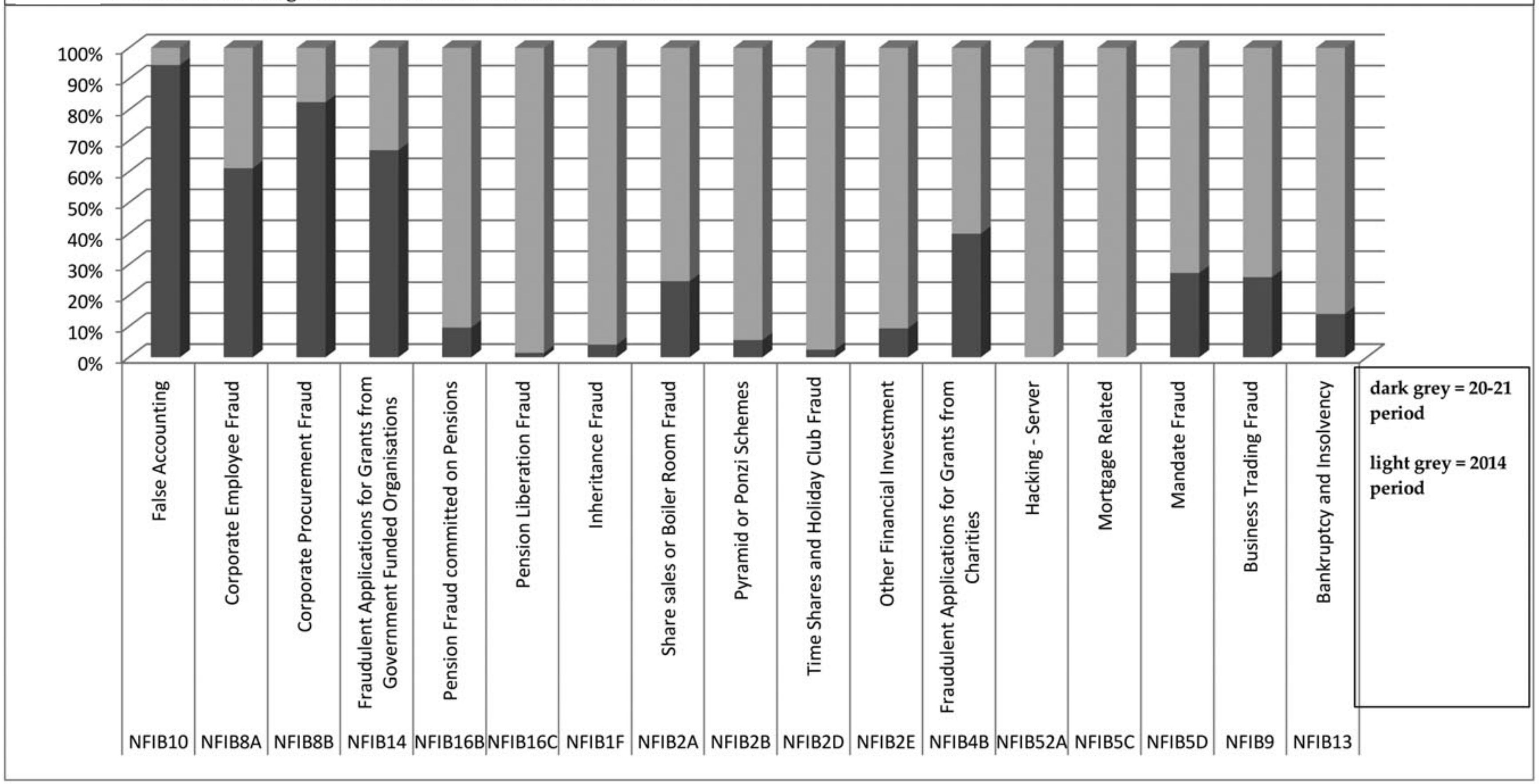
5.4 From AF to Dissemination to Outcome: A Snapshot

The Disseminations data does not carry the same richness of data as the AF data; the link is the criminal reference number (CRN). Given however, that cases reported during the AF data period (February 2020 to March 2021) were available for dissemination during the period of the Disseminations data, we cross-referenced the CRN, identifying cases whose progress we can see from reporting to AF, dissemination and outcomes. The majority of cases were as follows:

NFIB19 (Fraud by Abuse of Position of Trust):	31% of cases;
NFIB2E (Other Financial Investment):	4.5% of cases;

Part B - The Data:
Reports of fraud for the WMP area for May 2020 to July 2021

Table 13. +/- illustrative changes to median losses between 2014 and 20-21.



Part B - The Data: Reports of fraud for the WMP area for May 2020 to July 2021

NFIB52B (Hacking – Personal):	5.6% of cases;
NFIB52C (Hacking – Social Media and Email):	19% of cases;
NFIB5A (Cheque, Plastic Card and Online Bank Accounts [not PSP]):	6% of cases;
NFIB8A (Corporate Employee Fraud):	5% of cases;
NFIB90 (None of the Above):	9% of cases.

We analysed the variables on which we had data. 64% of cases came from the Birmingham (B) postcode area; the second largest (12%) came from the Wolverhampton (WV) postcode area. 80% of cases involved individuals and 20% organisations. The average age of victims was 49.5 years: 37% were aged between 25-49, 25 % between 50-69 and nearly 23% were aged over 70. In terms of ethnicity, 54% were white and 24% Asian. Over 72% had been prior fraud victims. 46% did not involve any recorded financial loss; this included 20% of the NFIB19 (Fraud by Abuse of Position of Trust) cases and 91% of NFIB52C (Hacking – Social Media and Email) cases. The total recorded losses were over £30 million; the median loss was about 0.02% of that figure, and the mean loss was 0.4% (showing the effects of a few very large losses).

Those categories with cases reporting losses over £100,000 from more than 4 cases were as follows:

NFIB19 (Fraud by Abuse of Position of Trust) – totalling over £2 million;
NFIB2E (Other Financial Investment) – totalling over £1 million;
NFIB5A (Cheque, Plastic Card and Online Bank Accounts [not PSP]) – totalling over £10 million;
NFIB8A (Corporate Employee Fraud) – totalling over £3 million.

NFIB90 (None of the Above) involved losses totalling over £5 million (most of which was associated with one case involving a potential loss of that magnitude but which to that point had only incurred an actual loss of £500,000, although there further projected losses of £30 million). One of the NFIB5A (Cheque, Plastic Card and Online Bank Accounts [not PSP]) frauds was a £10 million company fraud.
72.3% were identified as prior victims of fraud: but note that this does not mean that three quarters of fraud victims become repeat victims.

Of the cross-referenced cases, 3% resulted in a judicial outcome (primarily related to NFIB19 (Fraud by Abuse of Position of Trust) and another 3% were charged or summoned to appear in court, cautioned or were the subject of community resolution; almost 90% were not proceeded with.

5.5 PART B SUMMARY

The Action Fraud data underscores several points, particularly those that emphasise that fraud is not a homogeneous form of behaviour (and why it might be preferable to use the term 'frauds' to emphasise that variation), nor are all frauds equally harmful (although harm can be greater or less than economic loss), and nor are they all caused or perpetrated in the same way. Out of the 50 fraud categories and cases recorded by AF over a 14 month period, most of the specified (49) categories of fraud yield very low levels of reported cases: only 5 categories have more than 5% of the total of reported cases, all of which had median losses less than £500. Over 90% of reported cases involve individuals.

Some frauds impact more greatly on certain age and ethnic groups: specific groups, such as 70+, are disproportionally represented in particular categories. There were high levels of repeat victimisation among the fraud victims (although the data does not tell us whether for the same sort of fraud or over what time period). Some categories have particularly high levels of repeat victimisation, although the numbers of cases are low (except for Abuse of Position of Trust or non-PSP Cheque, Plastic Card and Online Bank Accounts). While the majority of cases and median losses are fairly even across the five WM postcodes, there is more variation between postcodes in terms of age, ethnicity and vulnerability.

Trends in the AF data for the WMP Area are similar to the national picture. Comparing the AF WMP data against national data from 2014, we can see both an overall increase in the number of cases and changes in their order of frequency. Cases involving NFIB5A (non-PSP Cheque, Plastic Card and Online Bank Accounts) and NFIB5B (Application Fraud excluding Mortgages) have reduced. On the other hand, investments scams, such as Boiler room frauds and Ponzi schemes, have increased. Online shopping frauds have markedly risen. These confirm that the internet has driven increases in some fraud types, though financial services sector efforts have prevented increases in fraud – in some cases quite significantly. Not adjusting for inflation, in only 4 categories of fraud have median losses increased, and most of those relate to business activity.

Finally, for the same period, but primarily not drawn from the AF data analysed, the NFIB disseminated over 1200 reports for investigation: in 14 fraud categories, no cases were disseminated. 6 categories accounted for some 60% of cases: 2 of those were also among the top 5 AF categories in terms of volume of cases. Of the cases disseminated to the WMP, over 60% were not pursued on grounds of evidential difficulties; just over 5% had a judicial outcome. In short, it appears that around 10% of reported fraud is likely to be triaged by the NFIB for dissemination. Of the disseminated cases, less than 5% will result in some form of 'objective' positive outcome. Overall, less than 1% of all fraud reported to AF is likely to end up being subject to a WMP investigation leading to a judicial outcome. Our analysis was not aimed at (or resourced for) allocating responsibility for this attrition, but these facts are an important background to thinking about what needs to be done to reduce fraud.

Part C - Discussion: Data issues and data findings

Discusses in 2 Sections the meaning of the data and what the findings say about fraud in the WMP area and how they relate to a public health approach

Part C - Discussion: Data issues and data findings

6. DATA MATTERS

6.1 The Importance of Data

Any public health approach is data driven. In the pandemic, improving data was a priority in assessing the impact of interventions as well as in judging whether the problems were getting better or worse. This is not always the case in policing and criminal justice, not only in England and Wales but internationally. In Section 2.4 above, we noted that the basis for a public health approach is the aggregation and interpretation of empirical data and the evidence base to ensure that interventions are designed, delivered and tailored to be as effective as possible. **It is important to appreciate that 'effectiveness' relates to the objectives of interventions, which can include anxiety as well as crime and collateral harms for first time and repeat victims, and even contested terms such as police legitimacy and national security.** Before looking in more detail at the interpretation of the data, following on from the narrative summary in Section 5.5 above, it is important to discuss areas for improvement in the data available. We have three concerns about AF's adequacy for profiling the 'fraud health' of the population.

6.2 Incomplete Data

The first concerns its variability and incompleteness as a basis for interventions. There are, for example, no data on victim gender, although there are for age and ethnicity. In some categories, the age of the respondent, ethnicity or reported value of the fraud is unreported or very incompletely reported (there are 5 NFIB categories with half or more entries of age missing, 17 with half or more value of loss missing, and 9 with over a third ethnicities missing). In the case of NFIB90 (no defined category), which constitutes over 27% of the volume of reported cases, 6% of age information, over 40% of losses and 24% of ethnicity information is absent. Such data might not be all that important for operational purposes, but they generate holes in the data for public health purposes (gender differences in susceptibility to fraud reduction techniques remain under-explored in the literature, except perhaps in romance or dating fraud). In some categories, over half the cases have no recorded value, including: NFIB13 (Bankruptcy and Insolvency), NFIB14 (Fraudulent Applications for Grants from Government Funded Organisations), NFIB3B (Consumer Phone Fraud), NFIB3E (Computer Software Service Fraud), NFIB4A (Charity Fraud), NFIB51A (Denial of Service Attack), NFIB5C (Mortgage Related), NFIB6A (Insurance Related Fraud) and NFIB8B (Corporate Procurement Fraud). In other categories, such as hacking, only a minority of cases specify losses (though this would be an illustration where the business cost of remediation might be much greater than the benefits to fraudsters). In the 'Hacking Extortion' – popularly described as ransomware – category, it appears strange that around 80% of reported cases appear to carry no value for what is essentially a fraud to extort money.

Where the frauds are known for serious loss (and harm), such as pension liberation frauds or lender loan frauds, an average of two-thirds of cases for the former and over 40% of the latter have no value specified. While we would prefer blank data to speculative/misleading data, these missing data raise difficulties for analysis. There are inherent difficulties in assessing some losses as arising from fraud rather than, for example, from trading losses in bankruptcy/insolvency frauds, both prosecuted and unprosecuted. Furthermore, profits from crime often do not equate to losses from crime: emotional impacts on victims bring no extra economic profit to offenders and though some offenders might get an emotional kick from deploying their skills, traumatised victims can bring extra 'heat' from the media, politicians and law enforcement. (Though sometimes this 'heat' takes the form of complaints of regulatory incompetence and demands for compensation rather than primarily for criminal justice.)

AF data and NFIB Disseminations data (which carries less data than the former) have some different characteristics, although they share CRN numbers. NFIB data has limited value in explaining victim risk, needs, vulnerability, etc., and NFIB offence categories are not sensitive enough to identify specific emergent methods by perpetrators. Neither dataset carries information on the levels and intervention points involving any cyber element to fraud that would assist prevention proposals. A key factor that would interest anyone seeking to analyse the Disseminations data – i.e., the reason(s) why the case was selected – is not included in the electronic data. This comes in a separate (paper) attachment with enhanced investigation information relating to the offence and those involved, including selection indicators, such as the involvement of an OCG or the amount of money involved, perhaps as a proxy for high harm.

Part C - Discussion: Data issues and data findings

6.3 NFIB90 and Repeat Victims

The second concern is categorisation of data in terms of being able to use for analysis. For example, over a quarter of the reports are allocated to a 'type' of fraud that is an unspecified residual, although this weakness is not (fully) replicated in the Disseminations data. Of the WMP AF data victim reports from May 2020 to June 2021, recording 50 different fraud categories in this period over 5 postcodes, the largest category is those frauds that do not fall into any of the pre-defined categories (NFIB90). Representing 27% of reports – the next is on-line shopping and auctions (the old-fashioned term that includes sales on eBay and Gumtree) at 24% – the NFIB90 entries are a very varied mix of cases but detailed examination of the narrative attached to some of cases suggests that a number would also be suitable for inclusion in other existing categories or new categories. The cases range from courier fraud, mandate fraud, account takeovers, identity fraud to employee theft, hacking, bogus traders and con artists, stolen goods and many reports of fraud attempts via telephone.

We are unable to clarify from the data whether 'repeat' applies to the same type of offence, to a range of categories, to the frequency and rapidity of the victimisation, or to multiple frauds within the same scam (such as escalating payments in a NFIB1A [Advanced Fee] fraud). It is clear that the ways the narratives are presented and/or the filtering mechanisms are complicating an already over-extensive category (this may also be true of other categories.) We are aware that AF will undergo a major revamp, but over the next few years something will need to be done about this missing data if the value of this database is to be realised.

6.4 Value and Loss: using Mean and Median

The third relates to loss and its representation. Of the frauds reported to AF, 12% of recorded frauds were valued at £100 or less and some 25% of reported frauds were valued at £1000 or less. While 30% had no ascribed value, nearly 14% had '0' allocated (and thus might have been failed attempts). Thus 81% of recorded frauds were £1000 or less; nearly 14% of cases were £1,001-£10,000; nearly 5% of cases involved amounts £10,000-100,000; and 0.5% of cases involved amounts £100,000-£1 million. We do not know the relationship between the nominal amounts defrauded and their impacts on individuals – the increasingly frequent media reports about fraud generally look for some sensational features or tropes to emphasise and to attract readers – but prima facie, this is very far from what one might expect from the portrait of fraud as a 'national security threat', though the numbers and proportion of the population subjected to attempted and even completed fraud is high, and this represents an insidious and harmful pervasive threat to the welfare of the general population.

Of the value of fraud, 61% of recorded fraud is accounted for by 17 cases (£1 million and over; or 0.075% of cases). These large cases represented a wider range of AF categories: NFIB90; NFIB2E; NFIB3D; NFIB5A; NFIB8A; NFIB3A; NFIB52E; NFIB2A; NFIB1D. Of these, three involved company fraud, two involved investments, three involved controlling behaviour relating to property (one was logged at 10x the value reported in the narrative). Two of the largest reported losses raise questions about the veracity of the claim (or the ability of the AF assessment process to verify the likelihood of the level of fraud taking place), given the nature of the allegation or interpretation by the AF recording process. Such figures skew the data. This is why we use median as well as mean values. Figure 2 and 3 illustrate variations by category and mean or median value.

Part C - Discussion: Data issues and data findings

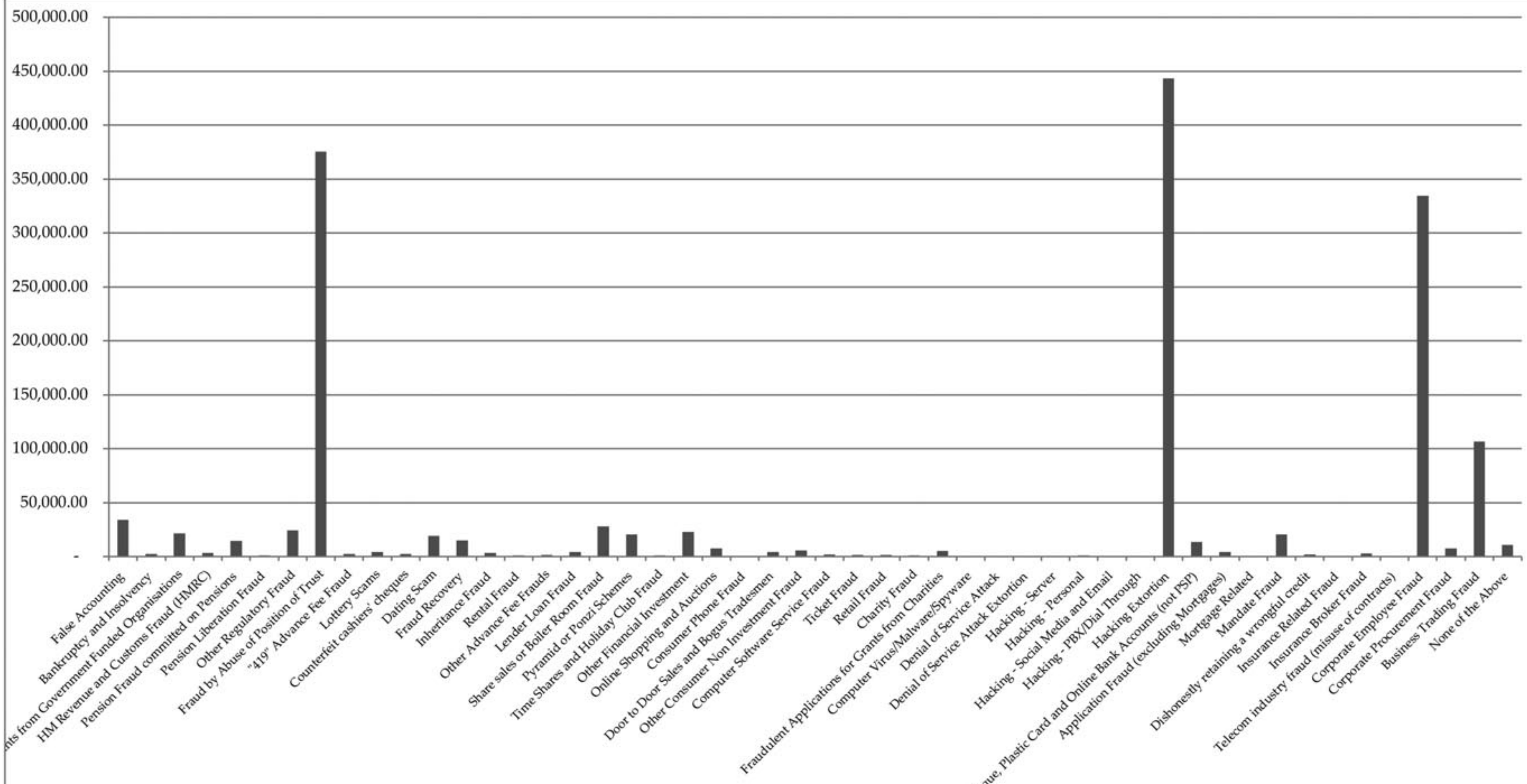


Figure 2. Mean value of Fraud

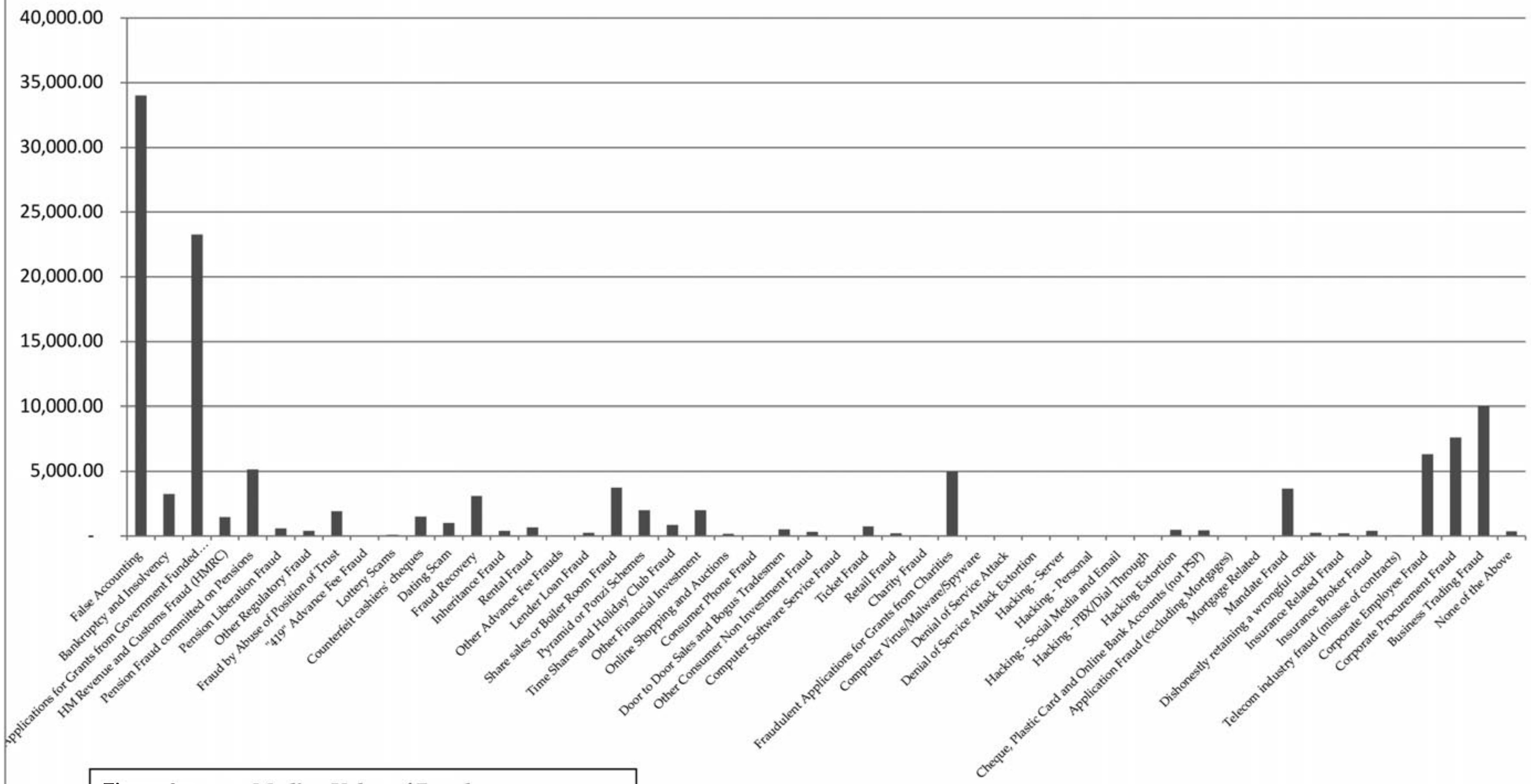


Figure 3. Median Value of Fraud

Part C - Discussion: Data issues and data findings

The obvious inference from the volume-value contrast is that most frauds fall clearly in the low-value/high volume area, and that areas of life where most frauds occur are not the same as those where the greatest losses occur (to both individuals and businesses). The fraud problems facing most of the population would not be those that (rightly or wrongly) would normally prompt police investigation: given scarce resources, investigations appear to be largely driven by being a linked series of cases and/or an Organised Crime Group (OCG) judged to pose an ongoing threat, the rationale for which judgment lies in information sent with but not part of the Disseminations dataset.

In the context of the stratospheric numbers generally quoted as the total cost of white-collar crime and money laundering, the individual cases and even the totals for fraud categories look somewhat modest and parochial. This does not mean that the losses are trivial to those experiencing them, however: one question for a public health approach (and indeed any rational policy) is whether lower economic value frauds should continue to be disregarded, and if not, what is to be done about them, whether by the police or by anyone else?

7. DATA FINDINGS

7.1 General

In recognising our concerns about the data in Section 6 above, as well as our concerns about transposing a public health approach without adaptation or development for a criminal justice context, it is illuminating to look in more detail at the picture provided by the AF data of who is affected by fraud generally and by what types of fraud. We can assess the levels, losses and variations by age, ethnicity, postcode and ‘vulnerability’.

We have examined some identifiable ‘fraud health’ problems in the population as reported by the public and organisations, disaggregated as far as possible by available variables, such as age and ethnicity. We have also considered the NFIB data which are disseminated to WMP: this represents the data that enters the equivalent of an Accident & Emergency department for triage for treatment/action/no further action. The implications of these data for interventions remain unclear, except inasmuch as the sheer volume of cases presents challenges for handling every type of fraud.

However, we wish to propose some initial steps in developing a public health approach: looking behind an issue or problem or illness to understand what might be driving it; focussing on prevention; proposing initiatives that reflect levels of intervention; and proposing partnerships and coordination as central because the breadth of population need and risk requires response (intervention) across many disciplines and services.

7.2 Losses and the Numbers of Untreated Victims of ‘Fraud Ill-Health’

In terms of the NFIB pre-defined fraud categories in the WMP AF data for May 2020 to July 2021, covering 50 fraud categories, most of the specified (49) categories of fraud yield – as noted above - very low levels of reported cases. 72% of cases of fraud reported to AF are generated by 5 categories but, as also noted, they have very low median losses. Similarly, the numbers triaged by NFIB for onward transmission are low at under 10% of those reporting to AF. In focussing on the general population’s ‘fraud health’ because the number being triaged and sent (though not necessarily accepted) for handling by the WMP are so low, the vast majority are entering a process where they are highly unlikely to receive any police intervention. For the most part, victims have no-one apparently explaining why they are not receiving any investigation, nor are they offered any alternative beyond basic fraud prevention information from the ‘Protect’ team, either immediately or – in cases being considered for NFIB dissemination – following the wait while a decision is being made to investigate or likely not. It is arguable that the median amounts suggest most are not suffering serious ‘fraud ill-health’, but many will also be repeat victims, and monetary loss is not the same as harm. Further, though we have little research evidence of their reactions many will presumably be left with feelings of both dissatisfaction and potential anxiety if they consider reporting frauds in the future (t the fact that many have reported in the past indicates that they were not put off by prior experiences.) The almost universal use of the internet and on-line financial services makes these consequences both highly likely and recurrent. There is a clear ‘fraud health’ issue that requires attention beyond law enforcement, whether or not it requires and receives more law enforcement attention.

Some 94% of reported cases came from individuals, the remaining 6% from organisations. Individuals are at high risk of fraud under all categories apart from the 9 categories which have primarily organisational victims (albeit with very modest numbers of cases, possibly reflecting business disillusion with the benefits of reporting frauds, though we have no data on why business reporting is low).

Nationally, in July 2022, AF is reporting over 400,000 cases of fraud, with losses over £3 billion: but this represents a mean or average loss under £7,500; the median will be much lower than that. For the AF data for the WMP Area, this low level of loss may explain why – unless the losses are identified as part of a series of such frauds, and are dealt with by the active ROCU or the ECU – most do not end up within the criminal justice process and are unlikely to result in any financial recovery unless they relate to card-protected shopping or online banking (where even then, half of victims who make claims are not compensated).

7.3 Findings: Age

The age profiles of victims change little across postcodes: though in CV, those under 24 are slightly more likely to be victims of fraud while in DY and WV, those aged between 50-59 are also more likely to be at risk of becoming a fraud victim.

There is some correlation between age groups and fraud categories, or between a greater level of reporting because of the likely vulnerability of the victim. On the other hand, that correlation does not necessarily extend to other categories of the ‘same type’ (such as financial frauds). The over 70s are less at risk than stereotypes would suggest, in relation to such categories as NFIB2B (Pyramid or Ponzi schemes). There are a number of other frauds where a significant number of a specific age group – other than the frauds against 70+ - are affected disproportionately: NFIB6B (Insurance Broker Fraud); NFIB1G (Rental Fraud); NFIB2D (Time Shares and Holiday Club Fraud); NFIB6A (Insurance Related Fraud); NFIB3E (Computer Software Service Fraud); NFIB16B (Pension Fraud committed on Pensions); and NFIB4B (Fraudulent Applications for Grants from Charities). The AF data does therefore show the potential for identifying the nexus of specific age groups and NFIB fraud categories where the number of cases and level of losses make prevention particularly important.

In accordance with what one would expect from routine activities models of crime risk, 70% of pension frauds concern those over 50, and two-thirds of victims in inheritance frauds are under 50. Certain frauds are more prevalent among expected age groups – nearly half of lender loan frauds are against the 25-49 age group - while others, such as lottery scams, show an equal distribution among the 25-49, 50-69 and over 70 groups. Dating scams, like online shopping and auction frauds, are more closely associated with those between 25 and 69: however, this is a very large age range, so it might be clearer to note that people 70 and over appear to be relatively less vulnerable to dating scams than the stereotypes would suggest. There are, however, other frauds where there is a significant number of a specific age group. Thus, those over 70 are disproportionately likely to be victims of a range of frauds: Door to Door Sales and Bogus Traders (NFIB3C), Fraud by Abuse of Position of Trust (NFIB19), and Computer Software Service Fraud (NFIB3E). There are also some identifiable crimes where the age group is likely to be a disproportionate victim, such as Time Shares and Holiday Club Fraud (NFIB2D) and Insurance Related Fraud (NFIB6A).

7.4 Findings: Ethnicity

The small number of victims for some sub-types should make us cautious about inferring relationships, but there is a positive correlation between ethnicity and vulnerability to particular frauds. NFIB6B (Insurance Broker Fraud), NFIB2E (Other Financial Investment) and NFIB3F (Ticket Fraud) are more likely to be more strongly associated with Asian or British Asian; NFIB2B (Pyramid or Ponzi Schemes) with Black or Black British; NFIB1F (Inheritance Fraud) with Mixed, NFIB16B (Pension Fraud committed on Pensions) with Other, NFIB3E (Computer Software Service Fraud) with White and NFIIB4A (Charity Fraud) with White Other. The AF data does therefore indicate the scope and rationale for preventive interventions with specific ethnic groups and categories of fraud.

7.5 Findings: Repeat Victims

42% of the victims have been previous fraud victims, so both percentage and absolute numbers make this a substantial target for prevention efforts. We wanted to know whether repeat victimisation differs by fraud category. Over a third of online shopping and auctions (NFIB3A) fraud victims had reported frauds previously. Disregarding missing data and the ethnic distribution of the population in the WMP area, 45% of online shopping fraud victims were white, compared to 27% Asian and 10% Black or White Other (and in line with the percent of population composition).

Cases involving substantial repeat victims are Cheque, Plastic Card and Online Bank Accounts (not PSP) fraud, Fraud by Abuse of Position of Trust, Hacking (Personal) and Door to Door Sales and Bogus Traders. When matched with the two higher levels of victim vulnerability, the most likely fraud categories targeting vulnerable repeat victims are: Hacking (Personal), Time Shares and Holiday Club Fraud, Other Financial Investment, Dating Scams, and Hacking (Extortion). These might be good candidates for public health interventions.

7.6 Findings: Postcode Variations

In order to determine whether the potential interventions are a force-wide issue or whether there are identifiable variations by the 5 postcodes, the research has reviewed the data against the findings in the previous Sections.

In terms of cases, and the distribution across the 5 main fraud categories by volume between postcodes, these show similar percentages. In terms of fraud categories outside the main five, there is consistency across the postcodes in further categories involving substantial numbers of reported cases; only one postcode appears to also have additional levels of risk in terms of NFIB1D (Dating Scam) and NFIB50A (Computer Virus/Malware/Spyware).

In terms of reported losses, the largest postcode by population was responsible for nearly 60% of cases, and accounted for 77% of the reported losses. One postcode accounted for 13% of the cases and 4% of the losses while others accounted for 8% of the cases and 4% of the losses; 8% of the cases and 11% of the losses; and 11% of the cases and 3% of the losses. One postcode accounts for 59% of the reported losses under NFIB5A [Cheque, Plastic Card and Online Bank Accounts (not PSP)] and 71% of reported losses under NFIB8A [Corporate Employee Fraud]. In terms of mean or average losses, the largest postcode had the biggest losses over 5 categories - NFIB52E (Hacking Extortion); NFIB19 (Fraud by Abuse of Position of Trust), NFIB8A (Corporate Employee Fraud), NFIB9 (Business Trading Fraud) and NFIB3C (Door to Door Sales and Bogus Traders). One category – NFIB8A (Corporate Employee Fraud) – was the only category to show consistent high losses over 4 postcodes; while NFIB19 (Fraud by Abuse of Position) occurs across 3 postcodes.

The 5 categories with the largest number of reported cases - NFIB90, NFIB3A, NFIB1H, NFIB3D and NFIB5A – have low median financial losses across all postcodes. Using median loses by fraud category over £1000 as a minimum level of loss, the assessment notes that some categories occur in all postcodes: Fraud Recovery (NFIB1E), Fraud by Abuse of Position of Trust (NFIB19), Counterfeit cashiers' cheques (NFIB1C) and Dating Scams (NFIB1D). Other categories are more post-code-specific. Thus, some categories involving financial frauds with median losses over £1000 - “419" Advance Fee Fraud (NFIB1A), Lottery Scams (NFIB1B), Inheritance Fraud (NFIB1F), Rental Fraud (NFIB1G), Other Advance Fee Frauds (NFIB1H) and Lender Loan Fraud (NFIB1J) – appear in three postcodes – CV, WV and WS – although not in B and DY postcodes. One postcode – DY – appears to suffer from frauds involving median losses over £1000 which do not occur in any other postcode: False Accounting (NFIB10); Corporate Employee Fraud (NFIB8A); Mandate Fraud (NFIB5D); Other Financial Investment (NFIB2E); Insurance Broker Fraud (NFIB6B) and Ticket Fraud (NFIB3F).

There were overall similar rates of repeat victimisation between postcode areas, averaging around 41%, though Dudley (37%) was slightly lower. We have not statistically controlled for this, but given differential populations in those urban areas, of those repeat victims, 61% are in Birmingham, 12% in Coventry, 11% in Wolverhampton, 8% in Dudley, and 8% in Walsall. The majority of fraud categories have 50%+ repeat victims across postcodes, with four – NFIB19 (Fraud by Abuse of Position), NFIB3G (Retail Fraud), NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)), and NFIB8A (Corporate Employee Fraud) - indicating high levels of repeat victimisation across all postcodes.

7.7 Findings: Fraud and Changes over Time

Fraud is getting more common, but the pattern of cases reported to AF is not changing so dramatically. Total reports to AF have risen over the years

Part C - Discussion: Data issues and data findings

(from nearly 73,000 in the year to March 2009 to over 200,000 in the year to March 2014 when our first analysis of AF data - Q4, 2014 - took place). Contemporary data shows that against 2014, the overall reported fraud landscape has not changed significantly, with NFIB1H (Other Advance Fee Frauds), NFIB3A (Online Shopping and Auctions), NFIB3D (Other Consumer Non-Investment Fraud), and NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)). NFIB90 (None of the Above) continuing to be the main fraud category by volume.

Within categories, however, there are some noticeable changes. Thus, likely because of better fraud prevention in the financial services sector, cases involving Cheque, Plastic Card and Online Bank Accounts (not PSP) and Application Fraud (excluding Mortgages) have dropped. On the other hand, investment scams directly against the public, such Boiler Room frauds and Ponzi schemes, have increased, as have online shopping and dating scams. The most striking changes are (i) the rise in the number of reported cases for the 5 main fraud categories by volume – and (ii) the percentage of fraud occupied by the NFIB90 category (None of the Above), followed by frauds strongly associated with increased Internet use (NFIB3A).

In the financial services and financial regulation areas (including pensions), median losses have dropped significantly, while the business and organisational sectors have seen substantial rises: the biggest median losses are associated with employee and procurement fraud, plus false accounting. By contrast, for the 5 main fraud categories, the median losses remain low (no higher than £500).

7.8 PART C SUMMARY

There were data problems that should be resolved if the data is to be used more constructively in a public health approach – whether the completeness and level of detail provided, or disaggregating NFIB90. Similarly, although more for understanding the triaging process, it would be useful to know the reasons for inclusion or exclusion in the cases disseminated.

The 'overproduction' of intelligence or information that cannot readily be used is not restricted to fraud.[18] For example, though they may be useful at a later stage for discovering offenders' assets, the number of Suspicious Activity Reports from regulated bodies in the UK is far too high to be investigated by the resources available, even with improved technology and Artificial Intelligence. The numbers of frauds being triaged to WMP from AF data are low, as are the outcomes of Disseminations. The criminal justice attrition – affected by low police fraud resources and capabilities – provides ample justification for arguing that the focus must be on prevention and reducing harm and damage, both to victims and to perceptions of how fraud is policed. Even if economic crime investigation resources in the constabulary, ROCUs and elsewhere (e.g., the City of London police and the National Crime Agency) were more plentiful and attrition less, we would still need to focus on prevention as the primary means of addressing the volume of reported cases.

The data reveal differences in victimisation by age, ethnicity, repeat victimisation or postcode, and these could provide the basis for developing a public health approach to addressing those levels of fraud and places where fraud occurs. With 42% of AF cases recorded as repeat victims – and some NFIB categories where all are repeat victims - then a focus on these is plainly appropriate.

[18] It is arguable that all information is good for analysing patterns and prioritising actions, but this is a broader debate about how to determine costs and benefits. See Levi, M. and Maguire, M. (2012) 'Something old, something new; something not entirely blue: Uneven and shifting modes of crime control', In Newburn, T. and Peay, J. (eds). Policing: Politics, Culture and Control, Oxford: Hart Publishing. pp.195-218.

Volume I

The West Midlands Police Area Fraud Report

Part D - Developing a public health approach to frauds

Concludes the Report with 3 Sections that discuss issues or constraints on adapting or developing a public health approach, then assess how far that approach may be developed within the context of the 4 Ps used by law enforcement to address Serious and Organised Crime, and finally what initiatives are promising to explore a public health approach to the prevention of frauds.

Part D - Developing a public health approach to frauds

8. PARAMETERS – ISSUES FOR DEVELOPING A PUBLIC HEALTH APPROACH

8.1 Using a Public Health Approach

The question at this stage is what we mean by adapting or developing a public health approach, particularly noting the caveats expressed earlier. There is a risk of mystifying the approach as something more radically different than it is. A public health approach differs from other types of crime prevention through strategic partnerships, problem-oriented policing or situational crime prevention because under a public health approach, it is understood that the police are no longer the lead organisation for community-wide prevention. Unlike other areas of problem-oriented policing, the volume and nature of frauds make it difficult for the police to develop a tailored 'solution' (particularly where the frauds are cyber-enabled), or develop many situational crime prevention methods, because many of the circumstances involve societal or personal behavioural nudges or changes. The police can and do promote fraud prevention through Protect officers' strategic partnerships, using their convening power (and raising money from the financial sector and from the Intellectual Property Office to pay for specialised units that focus on harm reduction and arrests in those sectors): but they will seldom be a lead agency as they are in spheres where criminal justice predominates as a way of dealing with criminal harms.

To some extent, it is moot whether this approach is termed 'public safety' or 'public health'. We recommend prevention-based interventions that have less to do with tackling offenders (though this remains an important plank of Serious and Organised Crime control) than an evidence-informed approach that aims to enhance the well-being and financial security of communities through a range of intervention levels. The potential stakeholders include government, law enforcement (primarily the police and trading standards, but also the SFO, BEIS and HMRC); regulators with some prosecutorial/administrative powers (the FCA, ICO, and Ofcom, but also the Pensions Regulator and the Payment Systems Regulator); cyber-threat reduction bodies such as the NCSC, the Global Cyber Alliance and GetSafeOnline; a range of for-profit and not-for-profit financial sector bodies such as CIFAS, the Insurance Fraud Bureau, Stop Scams UK and UK Finance; other sectoral bodies such as telecoms; and largely not-for-profit outreach Victim Support/Citizens' Advice/Consumers' Association/Age UK/Fraud Advisory Panel and technical/audit standards-setting bodies. Plus, a large range of for-profit consultancy/professional services firms.

This is a complex ecosystem to manage or referee, and it is not clear who does or could command central authority within it, as central Public Health bodies in the devolved UK governments seek to do in managing epidemics and pandemics. 'Fraud health' goals are about enhancing specific aspects of well-being. That approach will engage with community organisations and with counter-fraud public, private and third sector bodies (including health professionals): but it will also engage with the police for their deterrence and reassurance policing roles.

Several issues and policy dilemmas will affect such an approach. This research has undertaken a snapshot diagnostic of the 'fraud health' of the WMP Area. The first issue is what we do about the pervasive but often low-level nature of frauds as they affect the West Midlands community at large. Two points are worth noting here. First, being defrauded is the most common type of crime in England and Wales – administrative data show that scam calls have a very high incidence and prevalence: Table 14[20]. This is not a trend unique to the UK or West

Table 14. The Risks of Becoming a Victim of Fraud

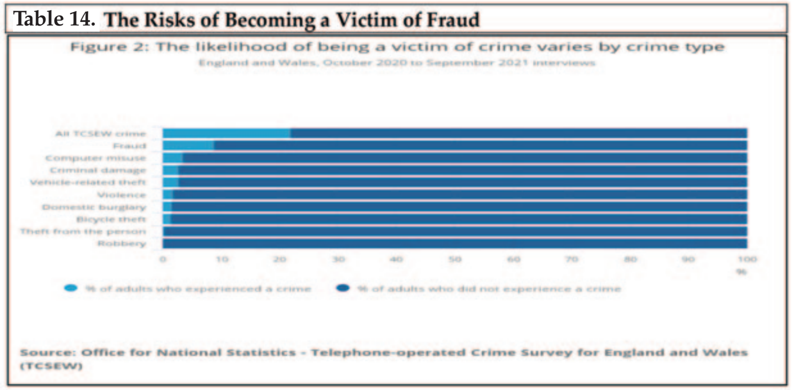


Figure 2: The likelihood of being a victim of crime varies by crime type

England and Wales, October 2020 to September 2021 interviews

Source: Office for National Statistics - Telephone-operated Crime Survey for England and Wales (TCSEW)

[19] See, more generally, Tilley, N. 2018. 'Privatizing Crime Control'. The ANNALS of the American Academy of Political and Social Science. 679(1). pp 55–71.

[20] A new CSEW is now available, and fraud is still top of the crimes but with fewer offences, and computer misuse remains in second place: but we have sought to use material as close as possible in time to the AF data. See also Correia, S. G. 2022. 'Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud'. International Journal of Population Data Science, 7(1): https://doi.org/10.23889/ijpds.v7i1.1721.

Midlands: other countries – such as the Netherlands - are experiencing substantial rises also, especially if we look at attempts.[21]

The second point to note is the attrition at every stage in the number of cases being brought into the criminal justice process (and 'brought to justice'). As discussed in both this and *Volume II: the Background Report,* data on the known and estimated scale of fraud perpetrated in England and Wales, the numbers of frauds in the large representative household Crime Survey for England and Wales (CSEW), cases reported to AF and cases disseminated by the NFIB for a police response, and criminal court/compensation outcomes shows a significant decrease at each stage.

Table 8 from *Volume II: the Background Report* for the WMP Area noted for the April 2019 to March 2020 period, over 18,000 AF-reported cases were distilled into 2,400 referrals, of which only 10% led to judicial outcomes – or 1.2% of reported cases. This attrition is not specific to the WMP area and nor does it appear to have changed significantly over time, perhaps because although police resources for economic crime may have fallen during austerity, they have never been anywhere near large enough to deal with even far lower fraud rates in earlier periods. When added to the increasing likelihood of becoming a victim of fraud, the relatively static number of fraud policing resources leads logically to the conclusion that the proportion of frauds processed through criminal justice will fall unless there is a dramatic rise in efficiency. It is not clear to us what such efficiency gains might look like and whether they are attainable, and this was not part of our research brief.

Our analysis of the AF data shows that the most frequent frauds have the lowest median losses. The rising 'cyber' components and case volumes may also suggest links to OCG activities or serial frauds seeking to accumulate value by multiple relatively minor payments, but the numbers (nearly three-quarters of all reported cases) are unlikely to attract individual attention from hard-pressed investigators. Further, as the AF guide for NFIB3A - Online Shopping and Auctions – notes, the transfer of funds means they are virtually unrecoverable with no recourse for the victim, whether that be the individual or their bank, despite the greater attention now paid to combatting money muling.

Interventions need to recognise the importance of awareness-raising, encouraging self-managed 'due diligence' and preventative 'treatment', including care and support, whose impacts need to be better understood. There may be large numbers losing relatively small financial amounts, but we know little about how much or little harm they pose to victims, nor about how much fear of fraud and alteration of lifestyle they cause. For most victims, excluding compensation provided by the financial services sector under the Contingent Reimbursement Model (CRM) Code and Banking Protoco[22], the likelihood of recovering their losses from offenders is very low, except where they have the means to sue authorised financial intermediaries or primary offenders successfully, occasionally with the assistance of litigation funders in mass victimisation or very high value cases.

8.2 Repeat Victimisation

The second issue from our analysis is the importance of recognising the high levels of repeat victimisation and considering how to 'treat' the harm and vulnerability of victims to prevent their future victimisation. In terms of reducing the harms done to 'vulnerable victims', the WMP AF data indicate that around 42% are repeat victims, so this is a substantial category (with 20 categories reporting that at least half are repeat victims). Over a third of online shopping and auctions (NFIB3A) victims were repeat victims. While some conscious or unplanned rationing of resource is inevitable, the WMOPCC should consider what levels of listening, care, counselling and support may be available for them, and who might provide more at what cost.

Situational crime prevention and the issuing of warnings without cognitive changes has its limitations. It would be helpful to differentiate between what we term spree offending (attacking multiple victims in one or more countries at the same time); serial offending (attacking the same or multiple victims over time); and repeat victimisation by frauds of similar and different types. These might be connected, e.g., via 'sucker lists' passed on to confederates or 'recovery frauds' in which victims are promised asset recovery by fraudsters who are likely to be part of the

[22] Levi, M. 2022. 'Frauds in digital society', In Housley, W. et al. (eds.). Sage Handbook of Digital Society. London: Sage.

[22] See CP22/4: Authorised push payment (APP) scams: Requiring reimbursement for a very recent consultation document on reforms to this process, reflecting the fact that in 2021, losses to APP scams totalled £583.2 million, a 39% increase on the previous year, though subsequent UK Finance data - 2022 half year update - show APP fraud losses fell 17% in the first half of 2022 compared with the same period in 2021.

same fraud network (whether or not they are formally classified as an OCG). But unless links to particular victims and/or multiple victims of the same offender are made (for example by social network analysis that includes common IP addresses, physical addresses and telephone numbers, or by Covert Human Intelligence Sources), such relationships will remain latent. The Insurance Fraud Bureau and private sector technologies can assist such Social Network Analysis (SNA) efforts at a cost, but we need to consider and measure what disruptive and preventive effects can be obtained in the aftermath of such intelligence.[23]

Further, from the data we have analysed, we cannot investigate the extent to which one-off and repeat victimisation may arise from networking by Ponzi or other fraudsters via affinity frauds (e.g., exploitation of religious or sporting affiliations). Nor, as we note from frauds elsewhere, are the explanations behind different regional rates of repeat victimisation obvious, e.g., early retirements and redundancy payments, as in the targeting of redundant Welsh British Steel private pension-holders by financial advisers, currently subject to police/FCA investigation and compensation.[24] It is possible that some of the suspect brokers and their contacts (including money launderers) reside in the West Midlands, but this cannot be deduced from the data on victims. The area requires more investment in data science analysts to connect potentially risky individuals, businesses, and professional firms/individual professionals to harmful events like frauds and phoenix company operations.

8.3 The Role of Gender

The third issue concerns the data composition from our perspective in terms of developing an evidence base. We have data on age, ethnicity and postcodes to inform intervention proposals, but as we noted in Section 5, victims' gender is absent. From research elsewhere, women are no more likely than men overall to be repeat victims of fraud, but the research may suggest that there are two male for every female repeat investment fraud victims, perhaps because (at least until the death of the male partner), men may typically have higher incomes and pensions/savings, and therefore have more to lose. There may be gendered differences in risk-taking. Further, according to the research, men may typically have much higher losses from most categories of repeat victimisation and men are more at risk than women from repeat fraud victimisation at a younger age.

The research also suggests that almost all the financial losses for female repeat victims occurred in the age groups 40-49 and 70-79, whereas men were more evenly spread out in age risks. Without more detail, it is not obvious why these younger age categories should turn out like this, and one should beware of drawing too much inference from small numbers. It seems plausible that if someone is scammed by a fraud recovery fraudster, they would have been scammed before – otherwise they would not be susceptible to 'help' at recovering their money – so all such victims might reasonably be regarded as repeat victims. The growing literature on romance scams suggests that women are more at risk at inflection points such as separation/divorce; the impact on men is less researched.

8.4 Understanding Risk Appetite

The fourth issue is insufficient knowledge of the spectrum of what we might term 'active' victims and 'passive' victims, based around attitudes to risk. A better understanding is needed of this spectrum of people who are 'up for' new areas of potential profit versus those who are highly risk averse. Both ends of the spectrum may be conned by being optimistic about the credibility of their information sources. FCA and other research suggest that levels of correct understanding of plausibly legitimate rates of return on investment are low, indicating the need for better financial literacy among adults and young people (and, in the view of this Report, at increasingly younger ages with access to their own or their parents' devices). In the contemporary world of truth decay, dire warnings from officials about crypto-currency value fluctuations and 'exit scams' may be disregarded by significant parts of their target audiences as the efforts of 'The Establishment' denying opportunities for ordinary people who are not part of the privileged inner circle. Unless the issue threatens to impact heavily the legitimate economic sectors, do such risk-takers who disregard warnings deserve a policing response if and when they lose money (the diplomatic resolution would be to make them low priority)?

[23] The Insurance Fraud Bureau, Cifas and suchlike bodies can reduce future fraud opportunities by denying insurance cover or credit facilities from their members unless controls are circumvented by false identities.

[24] House of Commons Public Accounts Committee. 2022. Investigation into the British Steel Pension Scheme. HC251. London: House of Commons. The FCA estimated they would pay out £71.2 million under the scheme, but this may be an underestimate. There are ongoing concerns: See https://www.ftadviser.com/pensions/2022/08/22/fscs-payouts-to-steelworkers-fall-by-30k/.

Part D - Developing a public health approach to frauds

Likewise, those engaging in what they consider legitimate activities, such as lender loans or (mostly online) dating where any consequential financial transaction may be highlighted by financial institutions as risky, but who are prepared to disregard warnings. Public health approaches generally try to pivot away from morality arguments about deserts, and towards advocating safer behaviour (and treating symptoms, however caused). This is fine for prevention efforts, but victims' deserts or (sometimes prejudiced) perceptions of deserts actually play a role in allocating Pursue resources, and taking the carefulness of victims into account is not inherently unreasonable provided it is not mere prejudice. Victims' self-blame and attempts to deflect accusations of recklessness and negligence is often part of the harm of fraud, as it is of sexual and domestic violence attacks.

As with many contemporary arenas of conspiratorial thinking, it is difficult to see who would count as an authoritative 'objective' source of information. Some would press for an appreciation of risk, risk appetite and acceptable risk mitigation measures, including more proactive or intrusive measures than have been undertaken by banks in the past, to try to stop people being foolish with their money. Some of these processes are now built into banking apps, requiring customers to sign off that they are not being pressurised etc.: data on the level of success of such measures is not yet publicly available. Likewise, efforts by banks to diagnose vulnerability individually or in categories, calling the police in to assist in dissuading people from becoming victims of courier and allied frauds. There will be police resource constraints to availability if such 'crime in action' measures are scaled up, but such calls for assistance are rare at present in the West Midlands.

8.5 Intervention Stakeholders

The final issue is to note that this project has not had the opportunity to undertake intensive interviews or surveys in relation to what victims may want or expect, from active intervention while the fraud is in progress to financial compensation or post-loss support and counselling. Though there have been no experimental exercises with control groups, the data we have from 2014 to the present – consistent with industry administrative data - suggest that active and concerted industry responses have reduced the levels of frauds in relation to specific fraud categories like payment card fraud: see Table 15. The absolute numbers as well as the proportions of fraud that these categories represent have dropped. Obviously, as with all crime reporting, the drop may not reflect underlying real crime changes: the long-lasting misuse of SIM cards to simulate other phone users (e.g., number spoofing) may not have fallen, and mortgage frauds and management frauds can take years before they are revealed. But some of these falls may be real.

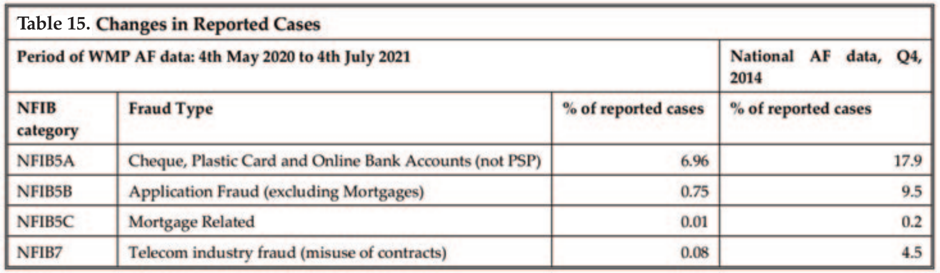


Table 15. Changes in Reported Cases

Period of WMP AF data: 4th May 2020 to 4th July 2021			National AF data, Q4, 2014
NFIB category	Fraud Type	% of reported cases	% of reported cases
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96	17.9
NFIB5B	Application Fraud (excluding Mortgages)	0.75	9.5
NFIB5C	Mortgage Related	0.01	0.2
NFIB7	Telecom industry fraud (misuse of contracts)	0.08	4.5

8.6 Prioritising Prevention Interventions

Serious questions need to be confronted as to what we want and what is feasible to get from policing in the range of activities coming under the label of 'fraud'. Decades ago, the WMP was actively involved in major fraud enquiries with specialist fraud prosecutors in the SFO and CPS: that no longer appears to be the case. It is superficially attractive to assert that prevention is the only goal of policing. Yet we do not apply that consistently in other spheres of policing in the WM area or anywhere else. A sense of justice for victims and for society, and (mainly the remit of the ROCUs and the NCA/NECC at present) the incapacitation of OCGs are also widely shared system goals (which aims to have some preventative effect on the accumulation of wealth and local/national power), as is stopping the flow of fraud proceeds to terrorists. Not all these demands can be satisfied.

It has become fashionable in the past year to advocate substantially more policing resources for fraud – and we agree that this is desirable for a range of reasons. But there is an element of magical thinking in some quarters, because the number of victims currently being given investigative assistance is so low as a proportion of the whole, and the forensic and cross-border issues in investigation and evidence provision (which lie beyond our brief here), combined with the dearth of experienced detectives and higher private sector salaries, insecure government finance for specialist units (though the current three year funding cycle is much better than the previous one-year one), etc., require some serious strategic thinking beyond past 'Economic Crime Plans'. Most cases of cyber-enabled, hybrid, and non-cyber fraud are fairly routine – the terms 'complex' and 'sophisticated' are over-used and ill-defined - but they take longer to investigate and require some different skill sets from other police cases. Basic fraud investigation skills need to be mainstreamed within 'ordinary' policing, because these are the normal crimes of today: but increasing resources for fraud investigations also has implications for clear-up rates for other crimes in a zero-sum resources model. It is not intellectually or socially acceptable to exclude most frauds in the West Midlands when we consider responses to 'neighbourhood crime', even though many offenders may not live in the same or nearby neighbourhoods. People are defrauded in their neighbourhoods using their smartphones or computers to buy, save and invest online; it makes no sense to exclude these from 'neighbourhood crime' simply because the offenders may not be from their neighbourhood.

Although there are good reasons to upgrade both the numbers and the percentage of policing allocated to fraud, what WM cases would or should an enlarged central or regional police take forward for Pursue? We have to be cognisant of available resources and the volume of cases set against the median loss per fraud type – and this requires strategic decisions on the balance between preventative and post-event measures. In the case of the NFIB90 (None of the Above) category the volume of cases, the variations within the category, and a median loss of under £450 might raise concerns about cost-effectiveness of post-event Pursue interventions (though so would many other non-fraud areas of police action[25]). Efforts to strengthen resistance to fraud by victims and third parties need to consider the fraud category or the platform by which the fraud is perpetrated, as well as balancing the responsibilities of the victim and the platform provider(s), as NFIB3A (Online Shopping and Auctions) and NFIB1D (Dating Scams) suggest.

9. DEVELOPING A PUBLIC HEALTH APPROACH WITHIN THE 4 Ps

9.1 A Public Health Approach within 3 of the 4Ps?

How far do existing efforts within the current 4 Ps (Prevent, Protect, Pursue and Prepare) framework for Serious and Organised Crime provide an appropriate platform for dealing with which frauds? And which components thereof might be part of a public health approach? Here, we only focus on those Ps which have a prevention element. Of course, we recognise that when taking down Internet servers or sites used in multiple frauds and undertaking 'Disrupt' tactics, Pursue adds to 'supply side' prevention, reducing via 'capable guardianship' the opportunity for future fraud (this is also part of the Protect role of the NCSC, where action against phishing is also part of action against cyber-enabled fraud, as well as against cyber-dependent crimes).

The public health approach might be popular as well as fruitful, especially in this (post?) pandemic/lockdown era where it is appreciated that mental well-being is an important but partly independent component from physical/financial harm. Thus, we might consider whether 3 of the Ps could be reconfigured to take a more holistic public health approach to 'satisfice' the public and potential and repeat victims with a not wholly scientific mix of general preventative measures (Protect), post-victim resilience (Prepare), and efforts to reduce the numbers and intensity of willingness to defraud (Prevent).

9.2 Protect

Our attempts to obtain a full account of the range of actual interventions currently deployed against frauds have not yet borne fruit. However, sufficient is discoverable about these efforts to outline them to assist in consideration of how best to address fraud in the UK from a public health perspective. As a 'health' issue, relatively little focused and/or evaluated effort has been extended by the public sector, and in some parts of the private sector, much effort has been extended in denial of culpability, especially by the mega-rich social media companies who have denied legal responsibility as publishers, even when they and Influencers

[25] This is too large an issue to be reviewed here, but it is difficult to apply cost-effectiveness analysis rationally to Pursue efforts. How do we specify the goals or benefits? Imagine the reaction if we officially declared that low value burglaries would not be investigated – though see Danny Shaw, 13 August 2022 https://www.spectator.co.uk/article/how-did-theft-become-effectively-decriminalised-in-britain.

Part D - Developing a public health approach to frauds

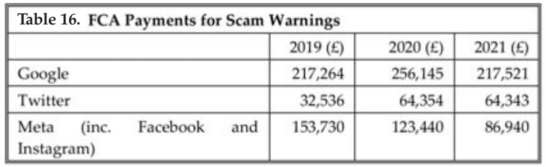


Table 16. FCA Payments for Scam Warnings

	2019 (£)	2020 (£)	2021 (£)
Google	217,264	256,145	217,521
Twitter	32,536	64,354	64,343
Meta (inc. Facebook and Instagram)	153,730	123,440	86,940

operating in their space have received payments from fraudsters[26] for running adverts on their own sites. Ironically, the FCA has spent over £1 million on those same companies delivering scam warning messages over the past three years: see Table 16. In 2019, the total across the three platforms was £403,531 and for 2020 this was £443,939. For 2021 it totalled £368,805.[27]

There is a risk that the scale of the problem can freeze us into paralysis when compared with the resources available to combat it. However, helping some people is better than helping none (or in this case, helping more people is better than helping the so far uncounted total of assisted fraud victims in the West Midlands. Victims who report to Action Fraud do receive general fraud prevention information by email: whether victims think this is adequate and its impact on future prevention is unknown and outside our research brief.) What we set out is what the evidence so far tells us about what has been attempted in the UK and elsewhere in combatting the kinds of frauds experienced directly by people and businesses in the West Midlands.

Much of the effort in Protect goes on in the background and some is more visible than others. There is a large ecosystem of counter-fraud bodies: both pan-industry (UK Finance, payment card schemes) and vendors for profit; not-for-profits (like CIFAS); government (National Cyber Security Centre, NHS Counter-Fraud Authority, the Public Sector Fraud Authority, and regulators such as the Charity Commission, the Financial Conduct Authority, and Ofcom). For example, efforts to warn the public of risks via formal advertising, media coverage of scams (currently more prominent than ever in tabloid as well as broadsheet press, radio and television), bank and card scheme activities in monitoring bank and payment card accounts and merchants for suspicious patterns of behaviour, telephone filtering services (like TrueCall or BT's Call Protect or Call Guardian) which only allow pre-authorised numbers to get through on landlines, and company internal and external audits (whose failures rather than successes are generally publicised). Telecoms components of scam schemes are finally beginning to be tackled more seriously, for example via the voluntary Telecommunications Fraud Sector Charter,[28] though they remain a work in progress.

There is a plethora of good advice on websites about the mechanics of fraud and what not to do: e.g. for a list of websites, https://www.met.police.uk/advice/advice-and-information/fa/fraud/useful-contacts-for-fraud-cyber-crime-advice/; https://www.getsafeonline.org/ (for general advice for individuals and SME business); https://www.ncsc.gov.uk/ (with separate advice pages for different business and individual sectors); https://www.fca.org.uk/scamsmart (especially for investment and pension scams); https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/ (for a wider range of doorstep to investment frauds); https://www.thinkjessica.com/; https://www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam/ (for consumers); and https://www.gov.uk/guidance/protect-your-charity-from-fraud (for charity frauds). There are increasing cooperative ventures, for example between Barclays, Cifas and GetSafeOnline for https://www.getsafeonline.org/checkawebsite/ which enables people to review the collective appraisal of websites' trustworthiness before they go to the website itself. The extent to which people actually do these checks is not publicly available.

In the classic 'fraud triangle' and its modifications, there are motivated offenders, suitable targets, and 'responsible guardians': much of situational crime prevention theory tries to strengthen the guardianship role, but fraud presents seductions that simpler crimes do not, and we need to be realistic about both the capacities and the motivations for

[26] It is not suggested here that they knew their advertisers were fraudsters.

[27] https://www.ftadviser.com/regulation/2022/01/26/fca-spends-368k-on-scam-warnings/. Google has subsequently donated a larger sum in free advertisements, which is welcome, even though this arguably is largely opportunity cost (for FCA payments foregone) rather than a real cost like the income it and others forego when they check claims of authorisation and then turn down the advertisement income if they detect that the claims are false. An increasing number of social media organisations have agreed to check the FCA website against advertisers before running the adverts.

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028171/Telecommunications_Fraud_Sector_Charter.pdf.

better guardianship. The debates over the coverage of fraud in the Online Safety Bill 2022, as amended, are a case in point. These have led to a new proposed standalone duty in the Bill requiring Category 1 and Category 2A services to take action to minimise the likelihood of fraudulent adverts being published on their service. This should make it harder for fraudsters to advertise scams online, and if Category 1 and Category 2A services fail to take adequate action the advertisers could face enforcement action. The government has included priority offences on the face of the primary legislation. This means Ofcom will be able in principle to take faster enforcement action against tech firms which fail to remove the named illegal content, rather than waiting for the offences to be made a priority in secondary legislation.[29] Whether this will happen in practice depends on resources and institutional will on an ongoing basis.

In the absence of the threat and/or actuality of anti-fraud provisions being addressed fully in the Online Safety Bill 2022 – and in the absence of media being prosecuted for laundering the proceeds of fraud when they are paid for advertising scams - there is little reason long term to expect all social media companies to deny themselves high profits from carelessly or even recklessly selling advertising and influencer spots to fraudsters and their intermediaries. It is not that they currently do nothing it all, but the economics of fraud control for social media companies differ from those applicable to payment card issuers and banks, who themselves pay for many of the material costs of fraud. Likewise, businesses that may sell counterfeit or fraudulently obtained goods on e-commerce marketplaces, which are now subject to greater controls than previously, but are still exposed in mystery shopping exercises by organisations like Which? Money and by investigative journalists. This mystery shopping should become a routine part of the fraud and money laundering regulatory process.

We can expect an increase in Protect focus from the FCA, using behavioural science insights:[30]

> Risk warnings that are more salient and informative for consumers, and informed by behavioural science, significantly increase consumers' comprehension and perception of the risks involved in high-risk investments. They also reduce consumers' propensity to recommend the investment to a friend and, if they do recommend it, they recommend a lower amount. However, these product-specific risk warnings can lead to unintended consequences on how consumers perceive other investments: in our experiment, participants' risk perception of stocks decreased when the new risk warnings linked to high-risk investments were shown.

This may benefit not just wealthier but also some poorer members of the public in the West Midlands, especially given the temptations of promised high yielding crypto-currency 'investments' at times when real interest rates are negative and inflation is higher than wage rises, sometimes supplemented by fake or genuine but paid-for endorsements from (in our view, mistakenly) trusted celebrities.[31] Historically, the FCA and its predecessors have not been proactive in warning consumers about investment risks, but a rising consciousness of fraud (and institutional media and political criticism for inaction in closing down businesses) have made them more active in 'fraud beyond the perimeter' of their authorisation processes, which themselves have been much-criticised for ambiguity and dilatory action. Predicting the future is difficult, and action against all but the clearest violations is more difficult but no less important!

The reshaping of victimisation patterns from the growing involvement of commerce in social media, especially in the Meta-verse via the rise in Influencers on Instagram and Facebook business adverts and apparent P2P recommendations. The National Cyber Security Centre has provided an easy process for individuals and businesses to report phishing emails (report@phishing.gov.uk), and paid-for advertising warns the public of the risks of clicking on emails. Most banking apps contain warnings against fraud, and many ask customers to confirm that they know the person(s)

[29] See, more generally, a helpful study by Westmore, K., Miller, S., Frost, J. and D. Foltean. 2022. 'Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams'. *RUSI Conference Reports*. London: RUSI.

[30] See Delias, D., Farghly, F., Hayes, L., Ng, C., and Spohn, M.. 2022. *Going beyond 'capital at risk': Behaviourally informed risk warnings for high-risk investment products*. London: Financial Conduct Authority; Farghly, F., Hayes, L., Ng, C., and Spohn, M.. 2022. *Pausing, reading, and reflecting: decision points in high-risk investment consumer journeys*. London: Financial Conduct Authority

[31] The Advertising Standards Authority has taken a commendable recent interest in controlling financial mis-advertising, but its powers are limited. London Transport, for example, has been slow to take down poster crypto-currency advertising. See https://www.theguardian.com/technology/2022/jan/14/cryptocurrency-ads-london-transport-tfl, which revealed that almost 40,000 crypto adverts were displayed on London Transport in a six month period.

Part D - Developing a public health approach to frauds

to whom they are sending money before they will allow customers to send money through the apps, et cetera. However, some customers disregard these warnings or treat ‘knowledge’ of counterparty more loosely than they should. One of the difficulties that both Protect (and Prepare) have is that an abstract awareness of how frauds work is not always translated into practice by targeted individuals when social engineering by practised fraudsters occurs.

Staff working in bank, building society and post office branches joined with the police to prevent customers from losing more than £45 million of fraud through the Banking Protocol in 2020. Under this rapid scam response scheme, branch staff are trained to detect the warning signs that someone is being scammed and to make an emergency call to the police. Police officers will then visit the branch to investigate the suspected fraud and arrest any suspects still on the scene. The extent to which there are glitches in police availability for this rapid response role to identified vulnerability is unknown but the more proactive banks are, the more strains this will create on limited police resource. Some banks have adopted a more active approach than others, also via anti-money muling teams to try to stop money laundering chains from moving the proceeds of fraud out quickly. Although these are costly investments, they may increase the reputation of banks and reduce the net profits of fraudsters. If some banks are more active than others, this may filter to fraudsters who will seek money mule accounts in the less vigilant banks.

The scale of fraud attempts is staggering. Ofcom research shows that almost 45 million people were targeted by scam calls and texts in summer 2021. Nearly a million (2%) of these consumers followed the scammers’ instructions, objectively (but apparently not subjectively) risking financial loss and emotional distress. Some fraudsters quickly adapt to controls and to technological opportunities. During the pandemic, for example, criminals were texting fraudulent vaccination links and impersonating delivery companies. Ofcom states that it has been working with other organisations on new ways to combat phone and text scams, and

> is proposing strengthened rules and guidance to combat number spoofing. All telephone networks involved in the transmission of a call will be expected to block numbers that are clearly spoofed. This rule would apply to all phone companies, ensuring the protection applies to millions of people…. sets out clear expectations for phone companies to make sure they run ‘know your customer’ checks on business customers. These could involve checking the Companies House register, fraud risk databases and the FCA’s Financial Services Register to uncover information that may indicate a high risk of misuse by the customer seeking to use phone numbers. Phone companies should also act to prevent any further potential misuse – this may include suspending the number and reporting evidence of fraudulent activity to law enforcement.[32]

When the entire phone system is digitised, proactive intervention will be quicker and easier: however, this will take years if it happens at all. Without cultural transformation in control efforts and a focus on the changing fraud environment, regulators will be insufficiently agile to keep pace, especially where the private sector is not actively cooperative.[33]

9.3 Prepare

In the Prepare space (a term not always understood by the general public), much is left to chance. The recent rise in ‘safeguarding’ attention to fraud victims is intermittent, though efforts are under way via Trading Standards to identify ‘vulnerable victims’ and to install TrueCall in their homes, which then generates data on levels of attempted fraud prevented via the number of scam calls cut out. In work done during the 1980s, Levi and Pithouse[34] showed that Victim Support and similar organisations almost totally neglected fraud victims, regarding them as capable of dealing with the experience and not as traumatised as burglary or ‘mugging’ victims; findings not much different in the much later research conducted in 2009 by Button et al[35] (and see Table 17).

32. https://www.ofcom.org.uk/news-centre/2022/crackdown-on-fake-number-fraud.
33. This can be a matter of interpretation, and ‘active’ is certainly a matter of degree.
34. Levi, M. and Pithouse, A. 1992. Victims of fraud, in D. Downes (ed.) Unravelling Criminal Justice, London: Macmillan.
35. Button, M., Lewis, C. and Tapley, J., 2009. Support for Victims of Fraud: An assessment of the current infrastructure in England and Wales, National Fraud Authority; Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. 2015. ‘'Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? The Howard Journal of Criminal Justice. 54(2). pp193-211.

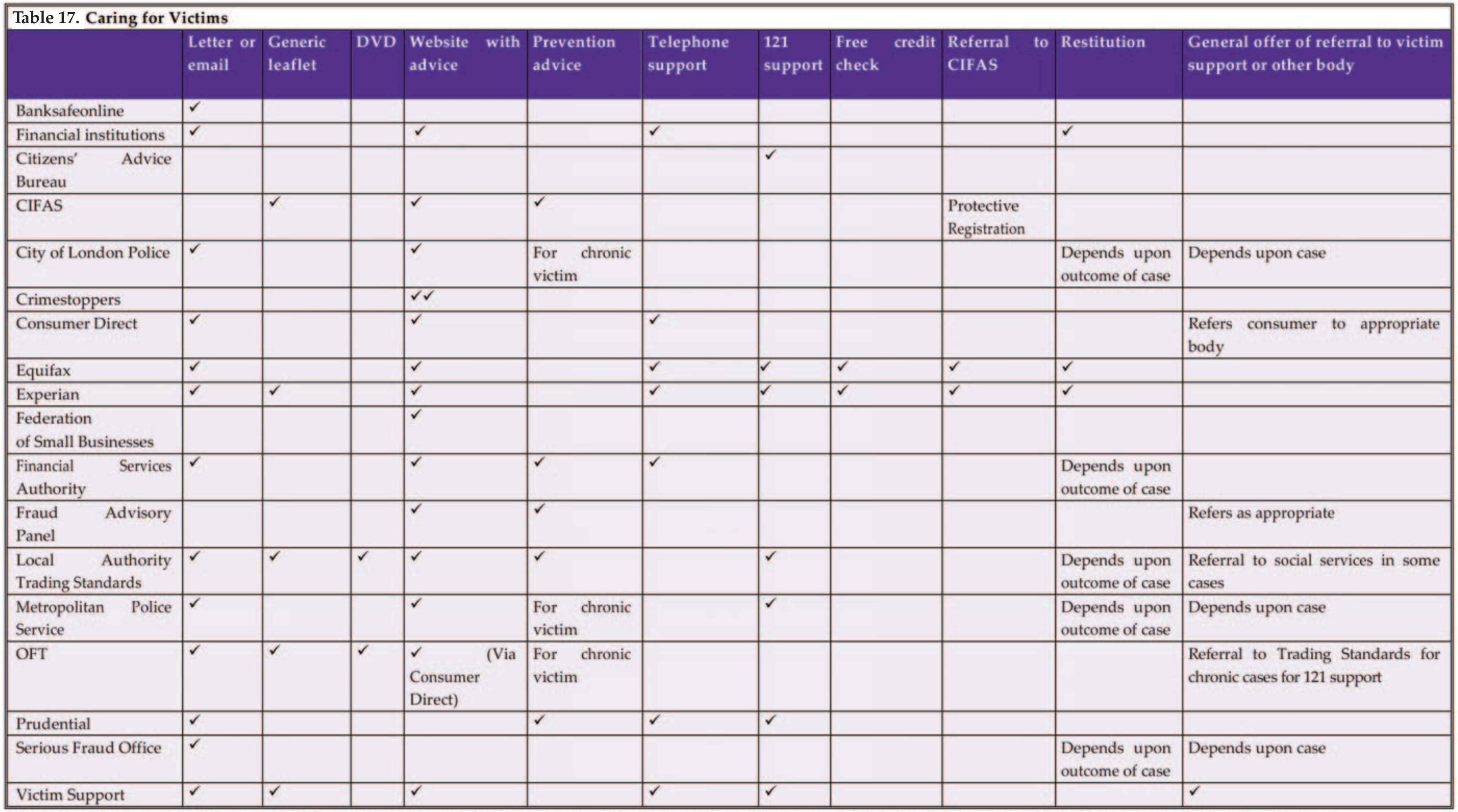


Table 17. **Caring for Victims**

	Letter or email	Generic leaflet	DVD	Website with advice	Prevention advice	Telephone support	121 support	Free credit check	Referral to CIFAS	Restitution	General offer of referral to victim support or other body
Banksafeonline	✓										
Financial institutions	✓			✓		✓				✓	
Citizens' Advice Bureau							✓				
CIFAS		✓		✓	✓				Protective Registration		
City of London Police	✓			✓	For chronic victim					Depends upon outcome of case	Depends upon case
Crimestoppers				✓✓							
Consumer Direct	✓			✓		✓					Refers consumer to appropriate body
Equifax	✓			✓		✓	✓	✓	✓	✓	
Experian	✓	✓		✓		✓	✓	✓	✓	✓	
Federation of Small Businesses				✓							
Financial Services Authority	✓			✓	✓	✓				Depends upon outcome of case	
Fraud Advisory Panel				✓	✓						Refers as appropriate
Local Authority Trading Standards	✓	✓	✓	✓	✓		✓			Depends upon outcome of case	Referral to social services in some cases
Metropolitan Police Service	✓			✓	For chronic victim		✓			Depends upon outcome of case	Depends upon case
OFT	✓	✓	✓	✓ (Via Consumer Direct)	For chronic victim						Referral to Trading Standards for chronic cases for 121 support
Prudential	✓				✓	✓	✓				
Serious Fraud Office	✓									Depends upon outcome of case	Depends upon case
Victim Support	✓	✓		✓		✓	✓				✓

Source: Button, M., Lewis, C. and Tapley, J., 2009. *Support for Victims of Fraud: An assessment of the current infrastructure in England and Wales*, National Fraud Authority.

Part D - Developing a public health approach to frauds

The now-defunct National Fraud Authority made a number of pertinent recommendations[36] but these may not have had much impact on practice, including:

> ‘in Action Fraud, victims now have a single place to report fraud, access practical advice and be referred to Victim Support – whose volunteers have been trained in meeting the needs of fraud victims’ (p6); ‘individual victims and small and medium sized businesses are now able to report fraud either online or by phone to Action Fraud. Online, telephone and face to face advice is available to help victims repair the damage caused and to protect themselves better in the future’ (p14); ‘now that we have a better understanding of the risk of fraud to particular segments of the population, we will monitor and evaluate the effect of targeted prevention messages on them. We will also work with the voluntary sector to use their networks to reach more vulnerable victims and potential victims’ (p19); and ‘we will expand the Action Fraud service so that it takes more of the crime and incident reports which currently are handled by the police, passes reports of incidents as well as crimes to the National Fraud Intelligence Bureau and takes reports of financially motivated cybercrimes and incidents. This will give victims a better and more consistent service and help them to avoid becoming repeat victims’ (p21).

The lead author of this Report has had subsequent discussions on fraud with some senior victim organisation office-holders with no observable changes following the NFA proposals.

One hypothesis is that until recently, most victim support organisations already had enough clients for ‘ordinary’ violent and property crimes without changing their practices substantially to deal with fraud victims.[37] Since then, the National Economic Crime Victim Care Unit (NECVCU) has been created to provide a better service to victims. After an initial pilot in London, the service is rolling out nationally. The NECVCU team has now expanded to a telephone service in the West Midlands and Greater Manchester.

The official website states:[38] “The Action Fraud National Economic Crime Victim Care Unit (AF-NECVCU) is a team of specialist advocates working within the City of London Police that supports vulnerable people who have fallen victim to fraud and cybercrime, with the aim being to make them feel safer and reduce the possibility of them becoming a repeat victim...The AF-NECVCU tailor advice to victims’ needs in a professional, sensitive and empathetic manner to support recovery and prevent re-victimisation through its core values; Engagement, Support and Empowerment...The team are not investigators and are only able to offer advice in respect to the recovery of any losses. The unit was set-up to provide a better service to victims, in the form of advice and support... NECVCU advisors contact people and offer advice but will never ask you for personal or financial information.” Little has been published about either the outreach or the impact of the NECVCU.

Victim Support note that out of 4.4 million CSEW reports of fraud that year (more now), “in 2019-20 we offered support to 7,074 people after they’d experienced fraud or forgery.” This is 0.16% of fraud incidents (not individual victims), and we have no knowledge of whether they were the most harmed or the most desirous of help among fraud victims. Although in principle, NEVCU is rolled out in 20 police areas (including WMP) covering 52% of Action Fraud reports, and it has been reinforced by funding from Lloyds Bank from assets frozen by its money muling teams, in practice it is implausible that serious emotional or practical support is given to more than a modest minority of even those victims who report to Action Fraud. Though there is an inevitable trade-off between repeated assistance and broader victim coverage, in our view, one visit might anyway not be enough to offer real assurance and check that

[36] In its last report; NFA. 2011. Fighting Fraud Together. London: Home Office

[37] For some good discussion of Australian online victim care approaches, see Cross, C., 2018. ‘(Mis) Understanding the impact of online fraud: Implications for victim assistance schemes’. Victims & Offenders. 13(6). pp757-776; Cross, C., Smith, R.G. and Richards, K., 2014. ‘Challenges of responding to online fraud victimisation in Australia’. Trends and issues in crime and criminal justice. 474. pp1-6; Cross, C., Richards, K. and Smith, R.G., 2016. ‘The reporting experiences and support needs of victims of online fraud’. Trends and issues in crime and criminal justice. 518. pp1-14.

[38] https://www.actionfraud.police.uk/economic-crime-victim-care-unit-ecvcu (Accessed 31 August 2022).

safeguarding arrangements are actually in place.[39] A further issue is, on what basis should scarce support be given, and is present service to victims based on more than a gut feeling about needs and deserts of different sorts of victims - for example, 'older people' or those visibly suffering? Earlier work showed the poor assistance typically given to those lacking mental capacity.[40]

[39] Our interviews indicate that repeat visits are the goal of some Trading Standards officers involved in safeguarding, and that they seek to assess the needs and vulnerabilities of scam victims, referring them to safeguarding teams in local authorities.

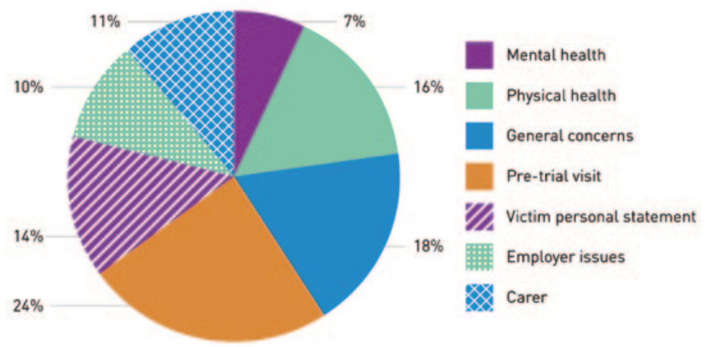
[40] Dalley, G., Gilhooly, M, Gilhooly, K., Levi, M., and Harris, P. 2017. 'Exploring financial abuse as a feature of family life: an analysis of Court of Protection cases'. Elder Law Journal 7(1). pp28-37; Gilhooly, M.M., Dalley, G., Gilhooly, K.J., Sullivan, M.P., Harries, P., Levi, M., Kinnear, D.C. and Davies, M.S. 'Financial elder abuse through the lens of the bystander intervention model.' Public Policy & Aging Report. 26(1). pp5-11. https://academic.oup.com/ppar/article/26/1/5/2593869/Financial-Elder-Abuse-Through-the-Lens-of-the#45685144.

Part D - Developing a public health approach to frauds

What sorts of needs are there and who is in the best position to give advice against repeat victimisation which, our data show, is commonplace? As the data in the Victims' Commissioner's report suggest, there is a need for a step-change in support. Their analysis found that though over half victims of fraud were not significantly affected, almost a quarter (22%) of all fraud victims – around 700,000 people a year – are likely to be deeply affected. They may experience very high levels of financial loss, severe emotional strain, including suffering from anxiety or depression and suffer relationship difficulties as a result of their being defrauded. Their report is less clear on the relationship between short term and longer term impacts, and on the predictive value of initial needs evaluation for those longer term impacts. In our view, though it might be difficult to identify who in the West Midlands area are the most vulnerable are at an early stage – and (to conserve scarce resources) to deny any assistance to those who are less than severely vulnerable – this would be an appropriate focus for care and safeguarding under the Care Act 2014.[41]

Some signs of progress may be found in recent initiatives by the Serious Fraud Office. An inspectorate report commended the SFO on its four-part needs assessment process that takes into account victims' and witnesses' changing requirements over the lifetime of investigations.[42] It was completed by 198 of the 285 witnesses the SFO was in regular contact with in 2021-22 and identified 112 needs – from mental or physical health to caring responsibilities – which the SFO is helping with. At the time of the review, only nine SFO cases had 'identified victims'. However, there are occasional cases involving thousands of victims, see Figure 4, so potential numbers are considerable: it would be a challenge for the SFO to meet all needs for them, let alone for the needs to be identified and met for all fraud victims in the West Midlands or the nation. The Victims' Code 2021 states that victims have a right to make a Victim Personal Statement and to be kept informed about the investigation and prosecution.

Figure 4: Breakdown of Needs Identified Among SFO Victims Surveyed



9.4 Prevent

'Prevent' is a term readily confused by the public who may associate it with general prevention rather than efforts to dissuade actual or potential offenders from crime. Other than professional ethics education and training – not hitherto a central feature of business schools or even professional associations – the only area where there has been any real policing effort has been in attempts by the NCA (and perhaps others) to divert those on the margins of cybercrime from criminal justice interventions. Prosecutions not only generate costs and effort to law enforcement but also might give younger offenders conviction or formal caution labels that might prevent them getting lawful employment in the financial services or cyber sector and therefore disincentivise them from going straight. Warning letters have been tried as a diversion strategy, and though reported to the lead author as an effective constructive shock for suspects, there has been little public evaluation of their impact.[43] The counterfactual would be difficult to assess because of the low visibility of cyber offending. In other spheres, there could be community-based efforts to turn young or older people in different areas away from engagement in frauds – online and/or offline (e.g. insurance crash-for cash) – and/or the closely connected money muling, but it is

[41] The Care Act 2014 s.42 and The Social Services and Well-being (Wales) Act 2014 place a duty on local authorities to make enquiries, or to ask others to make enquiries, where they reasonably suspect that an adult in its area is at risk of neglect or abuse, including financial abuse. The purpose of the enquiry is to establish with the individual and/or their representatives, what, if any, action is required in relation to the situation; and to establish who should take such action. The duty supplements the existing obligations on other organisations to look after the people in their care effectively, or, in the case of the police, to prevent and respond to criminal activity.

[42] *Victim and witness care in the Serious Fraud Office*. https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2022/01/20.12.21-SFO-Victim-Care.pdf. See also the *SFO Annual Report and Accounts 2021-22*, p.21.

[43] See Moneva, A., Leukfeldt, E. R., & Klijnsoon, W. 2022. 'Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners'. *Journal of Experimental Criminology*. pp1-28 (https://doi.org/10.1007/s11292-022-09504-2); Leukfeldt, R. and Jansen, J. 2019. 'Financial cybercrimes and situational crime prevention'. In Leukfeldt, R. and Holt, T. J. *The Human Factor of Cybercrime*. London: Routledge. pp 216-239).

not in scope for this modest study and impacts might not show up at the national level, given the scale of fraud.

It would be wrong to neglect the potential value of deterrent messaging in police and trading standards Pursue activities. They aim to communicate not just that fraud and scams are morally wrong but also that painful consequences will follow from involvement. This has most effect when potential offenders believe they have something to lose from detection. More systematic analysis of the ripple effects of such sanctions, including Serious Crime Prevention Orders sometimes imposed by the Courts, is needed. SCPOs should form part of a supply-side opportunity reduction strategy, though they can be applied only to convicted offenders.

At the other end of the spectrum, although the SFO is primarily an investigative and prosecutorial agency, its Deferred Prosecution Agreements and corporate monitoring schemes, like those of the FCA for money-laundering violations, can be expected to have some desistance impacts – rephrased by us as Prevent for existing serious economic offenders - though reoffending happens in corporate bribery and money laundering by firms under monitoring and post-monitoring. Some disqualified directors carry on business, using nominee directors to front the companies, though acting as a 'shadow director' is an offence. Enforcing such controls requires liaison between police and the Insolvency Service.[44] Again there are severe resource constraints within the Insolvency Service – which has experienced large cutbacks in recent years - and taking on contested high profile cases takes a disproportionate amount of funds and personnel, whether by the SFO, BEIS, the NCA or whomever.

9.5 3Ps Plus 2

In addition to possible approaches within the 3 of the 4 Ps, two further aspects may usefully be addressed. One is the question of restitution/compensation to victims – 9.5.1 - and the other – in 9.5.2 – is awareness of approaches taken outside the UK.

9.5.1 Compensation for Fraud Victims

One consequence of the growth of fraud and the complexity of its contexts is to place increased strain on civil compensation. This occurs in higher and lower financial bands. At the top band is the Financial Services Compensation Scheme (https://www.fscs.org.uk/), which guarantees individuals up to £85,000 per failed firm (including members of the same financial group) regulated by the FCA – this applies to failures due both to fraud and 'ordinary business', so there is no need to prove fraud. The Financial Ombudsman Scheme (FoS) also can require compensation where the firm has not gone bust.[45] This is not the place for an extended discussion of the FSCS or the FoS, but the limitations of both have been subject of formal reports and media commentary.[46]

In the lower band, the banks' compensation scheme – the Contingent Reimbursement Model - has also generated controversy, both in terms of whether card-holders have been negligent in failing to safeguard their PINs, and more recently especially as Authorised Push Payment scams have proliferated via social engineering. This can degenerate into compensation-by-media-shaming. There has been a failure to clarify consistently what the limits are, or should be, of victim entitlement when they have been duped. Some victims appear to think that banks are a general social insurance scheme to pay out for their errors of judgment, and despite pressures on non-member banks to sign up to the CRM model - it remains unclear how much diligence victims are expected to display to entitle them to be compensated, ultimately by shareholders and/or other customers of their banks (plus the taxpayer if that compensation is offset by banks against corporation taxes).

Another source of compensation is from the courts. The DPP notes that in the past five years, criminals have paid back £530m to the state because of confiscation orders obtained by the CPS, and almost £118m was returned to victims of crime in compensation.[47] Compensation therefore equates to £23 million annually. He advocates a change in legislation so that compensation as well as confiscation should be available in years to come if offenders are shown to have substantial assets, which appears to be a positive move. In addition to improving the care for economic crime

[44] Levi, M. 2008. The Phantom Capitalists, London: Routledge.
[45] https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams
[46] https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/
[47] The Financial Times, 19 July 2022

victims and witnesses, the CPS Economic Crime Strategy has as one rather general outcome: "proceeds of crime, both domestically and internationally, are recovered, depriving criminals of their 'ill-gotten gains' and compensating victims where possible."[48] If there is a rise in private prosecutions for fraud, note that under the Proceeds of Crime Act 2002, a private prosecutor can apply for a financial restraint order, to prevent the dissipation of assets and to preserve the position in anticipation of a post-conviction confiscation order, from which compensation can be paid.

This is a developing area, but where, to balance a public health approach, consideration may be given to a recognition that fraud involving individuals is mainly to do with economic loss arising for the most part from routine and everyday activities (akin, as one of those interviewed stated, as similar to driving cars – most of the time it's OK but sometimes 'accidents' happen). Here some form of integrated approach to compensation (not in the least in terms of eligibility) or insurance schemes that aim to maximise the opportunity or chances of compensation which most victims would want, particularly since criminal justice compensation rarely has much to offer. However, the conditions of entitlement and fear of promoting moral hazard may stand in the way of such models.

9.5.2 Learning from Elsewhere

Do any other countries handle frauds better? This is a difficult question to answer properly because it depends on legal systems including mutual legal assistance (for the Pursue function), on resources, on cultures of business and the professions, regulatory cultures, age/gender/ethnic distribution, inequalities and perceptions of fairness in society, levels of cyber-sophistication in the population, and other features related to fraud risk. There is no necessary connection between successful fraud prevention and fraud pursuit via criminal justice; nor between cyber-protection for ordinary citizens and that for large corporations who can buy in expertise. Appropriate learning depends also on what level of fraud one is seeking intervention on: the more routine volume scams, the high cost and largely off-line cases that might go to the SFO, or the high tech cases that might go to the NCA's National Cyber Crime Unit. The specific effects of asset forfeiture/recovery strategies on frauds have not been well examined to date.

The FBI and other US Federal agencies get the best publicity, and they do have the resources and political clout to throw at major cases and get mutual legal assistance (however much resented abroad at times): but several major corruption and fraud cases have failed in the courts there, and the US has a very complex ecosystem which may focus more on 'elder victims' than on general public protection. In 2017, 1.25% of all Americans 18+ reported that they were victims of personal financial fraud during the prior 12 months, and the repeat victimisation rate that year was 5% of them - only 14% of victims reported their frauds to the police.[49] In addition to these general fraud risks, however, in 2018, about 9% of US residents 16+ reported that they had been victims of identity theft during the prior 12 months.[50] Egregious large scale data breaches of personal and financial data held by hotel and retail chains and by financial services firms hardly suggest total success.[51] Canada has an anti-fraud centre (**https://www.antifraudcentre-centreantifraude.ca/index-eng.htm**) and along with standard 'what to watch out for' guidance online (e.g., **https://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7**), some programmes focused on senior citizens, but there does not appear to be any evaluation of their impact either on victim welfare or their risks of re-victimisation.

Australia has some good policing initiatives and scams surveillance: in addition to Scamwatch (run by the Australian Competition and Consumer Commission) and liaison between State-run policing and consumer protection units, these include the not-for-profit idcare (https://www.idcare.org/learning-centre/apps-and-tools).[52] But in 2020, 7% of the population suffered identity theft, though down from 11% in 2019; the lifetime identity theft rate was 19% in 2020, so it is arguable

[48] https://www.cps.gov.uk/publication/economic-crime-strategy-2025.

[49] Financial Fraud in the United States, 2017, https://www.bjs.gov/content/pub/pdf/ffus17.pdf.

[50] Identity Theft Supplement, 2018. National Crime Victimization Survey, Bureau of Justice Statistics

[51] https://www.upguard.com/blog/biggest-data-breaches-financial-services.

[52] Their website states: "IDCARE is Australia and New Zealand's national identity & cyber support service. Our service is the only one of its type in the world. We have helped thousands of Australian and New Zealand individuals and organisations reduce the harm they experience from the compromise and misuse of their identity information by providing effective response and mitigation."

that the scale of the problem there has driven better control initiatives.[53] The Dutch have a very competent Hi-Tech Crime Unit, and a thorough evaluation is planned for end 2022, but it is difficult to say how well the general protection works, given that in 2021 alone, 9.7% of the population were victims of online fraud,[54] a figure that is likely to have risen substantially subsequently.

Estonia has a good reputation for citizen-led cybercrime prevention, perhaps stimulated by the devastating Russian cyber-attack in 2007: local 'cyber-bobbies' help citizens with their protection. There is a French Francophone online platform called Signal-Arnaques that centralizes crowdsourced information about all kinds of scams and makes it available to its members. They receive more than a million visits a month and are using AI to process people's contributions better. They also rely on a mutual help model (victims helping victims).[55] This bottom-up approach may be more promising than top down initiatives for 'ordinary' risks. The UK, US, Israel, etc., have very good 'social' models for engaging business in the critical national infrastructure in trusted community information sharing for mutual benefit, via cyber-resilience organisations. There are also bodies such as the Global Cyber Alliance which act transnationally, and in 2022 announced a multi-agency Global Non-Profit alliance to reduce cybercrime risks.[56]

Consistently, the SME world is more difficult to help, since they cannot afford (or believe they cannot afford) the money or time needed for high cybersecurity skills, at least until they become victims. This is worrying since there is a trend towards targeting medium sized firms for ransomware attacks. Relatively little attention has been paid to offline fraud risks for SMEs, before or during the pandemic. We have not discussed the rise in ransomware, since our focus has been on fraud, but the NoMoreRansom initiative provides decryption keys to some strains of ransomware and brings together Europol, national police forces and cybersecurity companies.[57] Europol's EC3 cybercrime section has been particularly good at bringing together public and private organisations for online fraud as well as cyber-dependent crime, and Interpol has also prioritised this area of work to some effect. However, like most of the initiatives mentioned here, the focus has been on online fraud and cyber victims (plus anti-money laundering, which we have left out of this review): more 'traditional' offline frauds have been less of a feature, except in elder fraud in the US. International efforts have all been marked by the same absence of significant evaluation and outreach difficulties that has marked the UK. Namely although there are many sources of information online, including 'how not to' advice, it is unclear how many people look at them and take notice, or for how long they take notice and deny fraudsters opportunities when they do take notice.

9.6 A Public Health Approach within the 3Ps, or 3Ps within a Public Health Approach?

In looking at 3 of the 4 Ps (Protect, Prepare and Prevent), much of the effort in Protect goes on in the background and some is more visible than others. There is a large ecosystem of counter-fraud bodies, sometimes working in tandem but more often than not, specifically targeting their clients or customers. Much of this also involves the police, many of whose forces have Cyber Protect officers while some, such as the Metropolitan Police, have a Cyber Protect Team that was set up to help protect small to medium-size businesses and charities by providing advice, presentations and planning exercises with businesses and charities to raise awareness of cyber threats and help organisations protect themselves. There are also numerous websites and organisations offering advice: some data on website 'hits' are available, but the extent to which individuals and businesses follow through on them or on cyber essentials training (a precondition for public sector contracts in the UK) is not known. A data sharing capability has been developed by the National Cyber Security Centre (NCSC) in collaboration with industry partners that will present all UK Internet Service Providers (ISPs) with real-time threat data that enables them – but does not require them - to instantly block access to known fraudulent sites; browser and manager service providers will be invited to join at a later stage.

[53] McAllister, M. and Franks, C. 2021. Identity crime and misuse in Australia: Results of the 2021 online survey. Canberra: Australian Institute of Criminology.
[54] Dutch Safety Monitor 2021, https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021?onepage=true.
[55] https://info.signal-arnaques.com/. We are grateful to Professor Benoit Dupont for this reference.
[56] https://www.globalcyberalliance.org/cybersecurity-nonprofits-form-nonprofit-cyber-coalition/.
[57] https://www.nomoreransom.org/en/index.html.

Part D - Developing a public health approach to frauds

Bank, building society and post office branches joined with – and work with - the police for prevention through the Banking Protocol in 2020. Under this rapid scam response scheme, branch staff are trained to detect the warning signs that someone is being scammed and to make an emergency call to the police. This appears to have been used little in the West Midlands to date, but in principle, it is an excellent idea once staff are trained and the police can respond.

In the post-victimisation Prepare space, the recent rise in 'safeguarding' attention to fraud victims has been intermittent, and Victim Support organisations can only handle a modest number of cases as a proportion of fraud victims, not all of whom may need or want help in avoiding re-victimisation or reducing stress. Fraud may not be prioritised if there is a perception that fraud victims may be more capable of dealing with the experience and not as traumatised as burglary or 'mugging' victims. They certainly are not proactive in, for example, targeting repeat victims, while the end-to-end approach proposed by the National Fraud Authority in its 2011 report through AF has not had much impact on practice. Work published in 2017 showed the poor assistance typically given to those lacking mental capacity, while there is no linkage in the development of targeted tertiary interventions where repeat victims might raise their concerns initially with doctors' surgeries, Citizens Advice Bureaux, social care companies and so on and where these and other organisations, such as the WM Clinical Commissioning Groups (CCGs), to help identify and ensure that ongoing mental health services are available and accessible for at least some victims of fraud.[58]

Similar lack of focus and coordination may apply to 'Prevent' – where it is perceived as seeking to dissuade, for example, young people from cybercrime – and (under media and political pressure) compensation schemes, such as the banks' Contingent Reimbursement Model, have yet to clarify consistently what the limits to compensation are and what is the balance between customer responsibility and 'acting with reasonable care'. Indeed, one of the difficulties that both Protect and Prepare have is that an abstract awareness of how frauds work is not always translated into practice by targeted individuals when social engineering by practised fraudsters occurs.

We consider that there may be individual sub-components of a public health approach that can be learned from current 3P initiatives and those in other countries – especially from Australia.[59] We also acknowledge the importance of sharing between the equivalents abroad of Trading Standards and police, currently being attempted in England and Wales. This is taking place through the short-term funded MASH initiative between National Trading Standards and police, which may require more appreciation of local council and Trading Standards pressures and relationships to enhance its impact.

Data provided to us from the Dudley Trading Standards scams team show that extra staff recruitment – and especially the Financial Investigator - not only has an impact on arrests and victim recoveries of funds from 'rogue traders' but also on cost-effectiveness in reducing the numbers of elderly fraud victims taken into care homes in the aftermath of scams. They also provide fraud prevention advice and TrueCall landline phone services to some local residents on 'sucker lists' purchased by NTS. Other promising initiatives by Carmarthenshire Trading Standards are currently under evaluation. But there is no evaluated general model that can be copied for the full range of frauds that the West Midlands experiences. So in terms of conventional policy language, these count as 'What's promising' rather than 'What works'; and they may require a more stable approach to funding than a year-by-year one to ensure staff retention and focus on cases that may take years.

Overall, there is a plethora of interventions to combat and to reduce fraud (although we would argue, notwithstanding the perspective of the US centre for Disease Control and Prevention[60], that the level of the

[58] We appreciate that there is a chronic shortage of mental health services even without this proposed extension of their role. But this is not an excuse for disregarding the needs of fraud victims.

[59] Schemes for senior citizens in Canada and the US have been praised, but evidence of impact is lacking.

[60] 'The amount of a particular disease that is usually present in a community is referred to as the baseline or endemic level of the disease. In the absence of intervention and assuming that the level is not high enough to deplete the pool of susceptible persons, the disease may continue to occur at this level indefinitely. Thus, the baseline level is often regarded as the expected level of the disease...Epidemics occur when an agent and susceptible hosts are present in adequate numbers, and the agent can be effectively conveyed from a source to the susceptible hosts. More specifically, an epidemic may result from: a recent increase in amount or virulence of the agent; the recent introduction of the agent into a setting where it has not been before; an enhanced mode of transmission so that more susceptible persons are exposed; a change in the susceptibility of the host response to the agent, and/or factors that increase host exposure or involve introduction through new portals of entry' (https://www.cdc.gov/csels/dsepd/ss1978/lesson1/section11.html)).

'fraud disease' may continue to occur at current levels indefinitely and that total fraud prevention is clearly an illusory objective). If the police are to play a significant role in tackling frauds, the capabilities for dealing with the more routine cyber-enabled and offline frauds need to be mainstreamed more than they are at present. Even if there were a new 'economic crime force' accountable to, say, HM Treasury, the Home Office, Cabinet Office or another government department, it would not have the resource or perhaps the regional mind-set to tackle most of the low-level frauds experienced in the West Midlands or elsewhere. It is barely conceivable that it would have the resources to do so. Such national provision was envisaged when the SFO was created, but it is not currently resourced for this, and unless aggregated into larger cases (as the NFIB aims to do), low level frauds would not be within its remit of 'serious or complex fraud'.

Likewise, if the conception of fraud as a national security issue were adopted more seriously, the idea that this would extend to most of the frauds in the West Midlands we have analysed is fanciful, though it might indeed be applied as part of a serious and sustained effort to engage social media and other 'fraud enablers' in 'polluter pays' prevention and remediation of fraud. Though there are some long-standing fraud techniques which have been only partially prevented – there is always a temptation to focus on new methods of fraud and money laundering (like cryptocurrency scams) without addressing their proportion of 'the problem' - fraud reduction requires continual refreshment to handle new techniques and new constellations of criminals.

Overall, we consider that a public health approach would not function effectively within the 3 Ps, especially where there is relatively little systematic information about the rationale, choice, extent, forms and balance between the Ps in determining counter-fraud interventions or their effects, particularly not on their effects on levels of 'organised crime' and/or how frauds are organised.

10. INTERVENTIONS: RECOMMENDATIONS FOR BEGINNING A PUBLIC HEALTH APPROACH TO FRAUD

10.1 Overview: Whose Health?

Adapting or developing many of the current initiatives within the Serious and Organised Crime Strategy, in particular Protect, as well as some of the initiatives from overseas, would work better within a public health approach. This is for three reasons. First the approach focusses on the potential victims and their behaviour in terms of promoting generic awareness and due diligence on the part of the potential victim before undertaking a potentially fraudulent activity; second, it requires coordination between organisations and a streamlining of messages to ensure they resonate with particular groups or potentially fraudulent activities; and thirdly, there is a credible or trustworthy source, or sources, whose role in advice, guidance and support is known and easily accessible.

The public health intention is to improve the welfare of all individuals, and not just the small minority whose cases enter the criminal justice process. This involves taking a population level approach, a shift towards primary prevention, and a 'whole system' approach in developing responses. The public health approach is to aggregate and interpret the data looking at all the identifiable 'health' problems in the population as reported by the public, business and third party organisations, disaggregated as far as possible by available variables, such as age, geographic location and ethnicity. This would provide the evidence base to ensure that interventions are designed, delivered and tailored to be as effective as possible. Indeed, the point of a public health approach is to consider different intervention points, involving awareness and self-driven prevention and engagement with partners, businesses and others to reduce fraud. We start from a plethora of good advice, freely available online and offline, some of it produced by the West Midlands ROCU – *The Little Books of Big Scams* for individuals – and by the Metropolitan Police – *The Little Book of Big Scams Business Edition*; others have been produced and regularly modified by the NCSC, GetSafeOnline, Cifas, UK Finance, Which? Money, Martin Lewis' *Money Saving Expert*, et cetera. The scams and the warnings are dynamic. But though some fraud types fall (usually as a result of private-private or public-private partnerships, the energy for which is sometimes stimulated by legislation or the threat of it), the total frauds keep growing, so clearly there is a major outreach and impact challenge for which there is no current easy solution.

We noted in *Volume II: the Background Report* and in this Report that patterns of fraud victimisation and repeat victimisation are complex, and do not fit the stereotypes.[61] We should offer the majority of victims some service, with a particular emphasis on providing support to those whose losses and harms will not be triaged and promoting prevention and awareness to minimise the likelihood of becoming a victim – or repeat victim - of fraud, in the 'teachable moment' that may follow victimisation or near-victimisation - close escapes may sharpen the mind! Such measures need to be both widely publicised and continuing. Otherwise, the psychological and economic consequences of victimisation, the likelihood of repeat victimisation, and disappointed expectations in the face of inadequate support and law enforcement responses may impact more general perceptions of police (in)capability and (in)capacity to deal with fraud and other security concerns. There is no evidence about whether or not poor service for frauds will 'leak' into general perceptions of policing, but this consequence would not be surprising. The public may increasingly ask 'what are the police for?' if they believe that crimes to which many of them are subject – often repeatedly - seldom lead to any identifiable action.

10.2 Planning a Realistic 'First Steps' Public Health Response

Our starting point for a realistic public health response is that, based on our analysis of those reporting fraud to AF for the specified period, current and future victims of fraud will not receive significant support and care (even if their case is triaged by the NFIB for dissemination to the WMP). Recognising the complexities and dynamics of frauds as well as our incomplete knowledge of current initiatives, we consider that prevention is crucial for a number of reasons. As we have stated, some 90% reporting 'fraud ill-health' will not be selected for professional help of any kind beyond standard general fraud prevention advice by email. Given that this percent is not unusual and that frauds are increasing, it may be assumed that this trend will continue. Such cost-efficient advice may be taken up and found useful, but there are no public data on that or on its impact on future conscious or unconscious victim behaviour.

It is therefore important to explore what the data tells us about the types of fraud that are not selected and whether there is room for a greater focus on support, awareness and prevention to reduce the level of 'unsuccessful' reporting and harm. This – as we have discussed before – is particularly relevant in the cases of repeat victims and to reduce demand for or expectations of a law enforcement response. We note the high volumes and typically modest financial losses under certain NFIB categories. However, monetary loss is not the same as harm, and many will be left with feelings of both dissatisfaction and potential anxiety – or fear of fraud – if they undertake a similar action in the future, while others may take the view that 'life must go on' and perhaps continue as before, pledging to be more careful next time. Either way, there is a diverse 'fraud health' issue that requires non-law enforcement attention.

We have been able to collect, collate and analyse empirical data to develop an evidence base to begin to understand who are the victims, why they may be victims, and how frauds are perpetrated as well as to identify groups' propensities to fall victim to particular frauds. If taken further, this would allow recommendations that are focussed on prevention and on the promotion of partnership working across the community. We consider that we are beginning the discourse on developing a public health approach rather than implementing such an approach.

Our recommendations are drawn from the empirical evidence as proposals without the reorganisation of existing staffing, the agreement of potential partners or access to resources. The recommendations also relate to potential interventions not yet supported by evidence of effectiveness generated through trials or pilot studies, which would be assumed within the contemporary public health context. (Some recommendations will themselves propose what may be considered trials or pilot studies). However, we have to start somewhere, as public health practitioners did in the nineteenth century.

[61] See one good US longitudinal study: Deliema, M., Deevy, M., Lusardi, A. and Mitchell, O. S. 2018. *Exploring the Risks and Consequences of Elder Fraud Victimization: Evidence from the Health and Retirement Study*. Michigan Retirement Research Center Research Paper No. 2017-364/Wharton Pension Research Council Working Paper No. 2018-06. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1018&context=prc_papers - noted that when "responses were pooled across survey years, we found that younger, male, better-educated, and depressed persons reported being defrauded significantly more often. Victimization was associated with lower non-housing wealth....but had no measurable impact on cognitive, psychological, or physical health outcomes."

The approach will have to be both strategic and pragmatic: not all frauds can be addressed at the same time to the same degree of engagement. Given the volume of most types of fraud, discretionary implementation is inevitable. Much prevention work requires interventions at national level, possibly requiring legislative reform (as is being asked for in the Online Safety Bill 2022 and the Economic Crime and Corporate Transparency Bill 2022) or partnership working towards a more uniform response from payment and social media platforms, even when the pressure of prospective mandatory legislation eases. Such measures will have an impact on the WMP but are not something the WMOPCC can undertake on its own; they would require (at least) the Association of Police and Crime Commissioners (APCC) to act collectively at national or at least multi-force level.

In addition, not all fraud categories easily lend themselves to interventions. The 5 main AF categories may reflect the majority of cases, although not the higher end of median losses, which many take as a key indicator of harm and seriousness. The WMOPCC can do little by way of work on prevention or protection unless patterns and clusters emerge from deeper analysis of the data (in terms of unpicking in detail the narrative statements made by the victim). In other words, the total may suggest an epidemic or even a national security threat to public welfare, but we need more refinement of these frauds to respond appropriately. Similar concerns would apply to the other 3 main fraud categories by volume of cases. Thus, before proposing a comprehensive or WMP Area-wide public health approach to fraud, we suggest that the WMOPCC should initially be selective in testing the added-value and practicalities of the approach through some initiatives reflecting the three levels of public health preventative interventions.

10.3 A Public Health Approach: the Organisational Shape

The volume of frauds and attempted scams is large and socially significant, and to understand resilience better, we would do well to focus on frauds prevented, including by those who have not been victims, one-time or occasional victims, and repeat victims. Good awareness and advice on how to avoid fraud and good practice on care and support abounds: the problem is to organise, resource, coordinate and communicate through an organised public health approach in such a way that people listen, remember and apply it ’in the moment’. The challenge is to balance an outgoing mind-set with an appropriate level of scepticism and improved financial literacy, which should begin early in life, even at primary school given the spread of smartphones to people of that age. Clear guidance needs to be developed and communicated on where to get help before and, for potential repeat victims, after first-time victimisation.

While recognising that a number of elements to such an approach are absent (for example, data on gender or levels of risk appetite), in terms of adapting or developing a public health approach, the perspective we recommend are prevention-based interventions that have less to do with tackling offenders[62] than an evidence-informed approach that, like public safety, is about the well-being and security of communities but, more like public health, is about specific aspects of that well-being as denoted by promoting ‘fraud health’ through prevention measures. That approach will engage with community organisations and with health professionals but will also engage the police both for their deterrence role and for the provision of public reassurance that their concerns may be being paid attention to, depending on the seriousness of the ‘fraud ill-health’ (of course, this is not an argument against increasing police resources to increase fraud disruption and justice for victims: it is an argument for a broader attack on fraud).

Evidence-based medicine might not regard such ‘reassurance policing’ as a worthwhile investment unless it also reduced victimisation or mental ill-health. Interventions are intended to strengthen resistance to fraud by victims after considering the fraud category or the platform by which the fraud is perpetrated, as well as balancing the responsibilities of the victim and the platform provider(s). Interventions need to recognise the importance of awareness-raising and preventative treatment, including care, guidance and support. There may be large numbers losing relatively small financial amounts but causing non-trivial levels of harm to those involved, plus generating fears of fraud. Similar concerns apply to repeat victims.

[62] Some approaches to deterring online offenders are reviewed in Volume II: the Background Report. See also somewhat promising warning emails sent to online romance fraudsters - Wang, F., Howell, C.J., Maimon, D. and Jacques, C. 2020. ‘The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach’. CrimRxiv, November 5. https://doi.org/10.21428/cb6ab371.c6eae022.

Part D - Developing a public health approach to frauds

As Table 18 suggests, there are a number of organisations seeking to prevent fraud and to support victims of fraud; there are also a number of organisations likely to know of victims of fraud. These range from those dealing with financial frauds and scams (see 9.2), the social sector including Age UK, Citizens Advice Bureaux, faith organisations, the Samaritans, social services, and so on, and organisations from the health sector, such as GPs, social care, CCGs and mental health charities. There are organisations that can offer specialist advice and support both to victims of fraud and those who fear to become victims of fraud. This project has not had the opportunity to conduct in-depth analysis, but we are aware from our other research that this patchwork quilt of support is under strain, and there is little research evidence that law enforcement's approach to and resourcing for Protect and Prepare is or is not particularly impactful. (Apart from the status and powers of office, it is not self-evident that serving officers are best placed for such work). We have not examined the impacts of counter-fraud marketing or social media campaigns in the WMP Area, but such campaigns to date have not received serious public impact evaluation: showing that one is 'doing something' is not enough to meet the evidential requirements of a public health approach. At the same time, the diverse and unstructured nature of some sectors, such as education, suggests the importance of a common liaison or coordination role (thus for education this would include engaging with the DofE, Heads and Governors as well as Trusts, especially MATs, Multi Academy Trusts). Finally there are a number of lesser-known bodies that could act as a conduit into specific sectors, such as Business Improvement Districts (BID) which have huge opportunities to support local businesses with the type of initiatives we are proposing.

We therefore see an important leadership, coordinating and organisational role for the WMOPCC in proactive pursuit of fraud, not only to bring together all relevant organisations and expertise but also to make strategic and financial decisions appropriate to the level and type of intervention. For any initiative based on the AF data in terms of volume, median loss, age, ethnicity, repeat victimisation and postcode, the WMOPCC needs to pull together the various groupings above to assess: current work and overlaps; appetite for engagement; current initiatives or initiatives elsewhere that may be applied to the WM Area; and enthusiasm for working together on a prevention strategy, key stakeholders and a limited number of initiatives to deliver a holistic public health approach in practice. This will require refinement according not only to what is currently in place, involving assessing what is the added-value of WM OPCC involvement to which elements of counter-fraud, but also the extent to which affinity groups or coalitions of the willing can be aggregated together in a sustainable fashion if the WM OPCC agrees its specific strategic approach[63].

If the implementation of the ownership and coordination role is positive, then our recommendations and potential initiatives are the first step in trialling what might work in practice and bringing together those who may add value in preventing fraud. To do so can only benefit the 90% of victims who report to AF in the WMP Area but who do not benefit from engagement with the WMP (plus the many non-reporting victims and future victims who may be helped by better fraud avoidance help). The WMOPCC has the opportunity to lead on undertaking a public health approach alongside the law enforcement work. In so doing, it can seek to prevent and reduce the demands on, and away from, the WMP and the Pursue function, while stimulating guidance, care and support necessary to those whose losses and harms will not realistically be addressed. Frauds of many kinds are unlikely to go away naturally: these risks that affect many of our lives will always need to be managed and mitigated.

10.4 Initial Intervention Initiatives

We contend that the organisational framework should precede any initiative to assess the adaptation or development of an initial public health approach in practice based on their collective response based on the clusters of fraud 'ill-health' by NFIB category, age, ethnicity and so on which would fall within the criteria for public health approach interventions. Consideration should be given to whether these should be new initiatives or integrated with existing ones, although the WMOPCC would also be well-placed to address this, given our proposals for its strategic role. There currently is no clear published mapping of what is done to and from what sorts of fraud victims by whom.

[63] We suggest that the WM OPCC may wish to consider branding the overall initiative with a defining label such as the 'WM Fraud Health Hub'.

Part D - Developing a public health approach to frauds

Without pre-empting choice, it is expected that the organisations involved would wish to see what the initiatives could be in order to assess levels of engagement, resources, added-value and evaluations. Though this enterprise is a long term one, we propose 5 short-term initiatives.

10.4.1 Volume Fraud, Low Value and General

Initial Initiative 1: primary and area-wide: apart from NFIB90, four other categories dominate the AF data: Online Shopping and Auctions (NFIB3A); Other Advance Fee Frauds (NFIB1H); Other Consumer Non Investment Fraud (NFIB3D); Cheque, Plastic Card and Online Bank Accounts (not Payment Service Provider (PSP) (NFIB5A). All involve the need for the promotion of awareness and caution by potential victims, whether paying for goods and services or guarding financial details and instruments. In most cases, the amounts involved and the likelihood of recoverable expenditure are variable, and with only around 3% likely to be included for dissemination (and even less for criminal justice outcomes), there is limited recourse for the victim, although there is potential for a greater use by law enforcement for intelligence purposes or for looking for OCGs behind multiple victims.

Something more clearly needs to be done about the ubiquitous risks posed by growing social media declared and undeclared advertising of risky investments. Given the amount of attention that scammers are getting daily in social media, podcasts, Netflix-type streaming series, radio, TV and the press, it is telling that many people are unaware of some fraud risks: but media coverage focuses on the more sensational cases, as it does for other types of crime. Media and social media campaigns might raise awareness of scammers' techniques as well as the harms of frauds[64]: but the Take Five and other campaigns have already been in place and the in many ways excellent FCA 'ScamSmart' campaign – on which millions have been spent – has had modest numbers of visits and little demonstrated impact to date. Nevertheless, it is desirable to mount a public campaign across the WM Area involving financial services and other institutions, including information on risk and sources of advice and guidance as well as a crafted message underlining what the police and trading standards can and cannot do in the event of a fraud. This needs both qualitative and quantitative evaluation indicators.

10.4.2 Targeting Repeat Victims

Initial Initiative 2: tertiary and individual: Table 18 reprises the data on those fraud categories that elicit significant levels of repeat victimisation. To put this in context, the most recent published Crime Survey has repeat (50%+) victimisation rates of 22% for bank and credit account fraud, 16% for consumer and retail fraud, and 26% for other frauds measured[65].

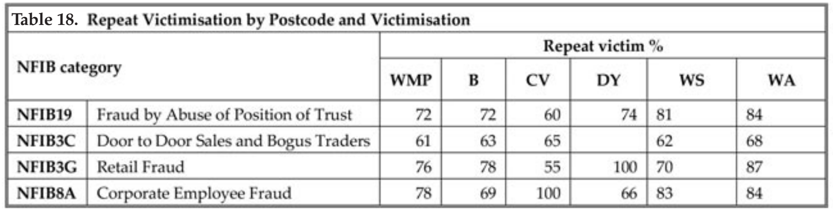


Table 18. Repeat Victimisation by Postcode and Victimisation

NFIB category		Repeat victim %					
		WMP	B	CV	DY	WS	WA
NFIB19	Fraud by Abuse of Position of Trust	72	72	60	74	81	84
NFIB3C	Door to Door Sales and Bogus Traders	61	63	65		62	68
NFIB3G	Retail Fraud	76	78	55	100	70	87
NFIB8A	Corporate Employee Fraud	78	69	100	66	83	84

We know that NFIB3C (Door to Door Sales and Bogus Traders) stands out in terms of losses and number of cases for the Birmingham postcode and we also know that those over 70 are disproportionately likely to be victims of NFIB3C frauds. It is unclear whether those victims are repeat victims for the same or different fraud types, but AF has recorded high per cent levels across the WMP Area for these categories. Given the organisations involved in supporting victims, and the relatively small number of reported cases (just over 600), we recommend the creation of an operational unit of relevant organisations to proactively approach victims or focus on NFIB3C in the Birmingham postcode to test the demand and nature of the support needed to prevent repetition of susceptibility to fraud.

[64] While a number of sites, such as Amazon and eBay, are quick to refund victims of fraud if they have conducted their transactions within their payment bubble, their anti-counterfeiting efforts are more complicated to assess, though recent pressures have led to more action. In 2020, only 6% of attempted new seller account registrations passed Amazon's verification processes and listed products for sale. In addition, fewer than 0.01% of all products sold on Amazon received a counterfeit complaint from customers: https://press.aboutamazon.com/news-releases/news-release-details/amazon-counterfeit-crimes-unit-reaches-settlement-influencers. Amazon claimed it blocked 10 billion phony listings in 2020: see https://www.nbcnews.com/tech/tech-news/amazon-blocked-10-billion-listings-counterfeit-crackdown-rcna875

[65] Table D8, telephone-operated Crime Survey for England and Wales, Year ending March 2022

Part D - Developing a public health approach to frauds

Here we would envisage targeted tertiary interventions where repeat victims might raise their concerns – doctors' surgeries (notwithstanding the strains upon them), Citizens Advice Bureaux, social care companies and so on and where these and other organisations, such as the WM Clinical Commissioning Groups (CCGs), may help ensure that ongoing mental health services are available and accessible for at least some victims of fraud. Conversely, such organisations should have a means to collate and coordinate identified vulnerable or repeat victims' support and supervision. Some particular vulnerabilities – for example the increasing numbers of people lacking mental capacity (or who have declining mental capacity – in our view, a less binary and more useful way of categorising for operational purposes) – may be given special treatment or focus. They are at risk not just from strangers but from family and friends, and even from licensed professionals and trusted persons and organisations. This is one of many challenges facing safeguarding.

We would also return to the proposals of the 2011 National Fraud Authority report and recommend that AF – on receipt of a report from a victim flagged up as a repeat victim – sends out an email of the contact details of these organisations and – perhaps with a victim-determined opt-in or opt-out – an indication that they can or will contact them to provide support. This would address individual levels as defined by priorities of harm and vulnerability, while engaging in tertiary prevention to help them through counselling or support groups to manage their vulnerability to becoming repeat victims. It would supplement the standard fraud prevention advice currently sent out to victims.

10.4.3 Targeting Specific Groups

Initial Initiative 3: primary and group/community: Under-24s are disproportionately more likely to suffer from NFIB6B (Insurance Broker Fraud, where victims obtain insurance cover from a broker or someone purporting to be a broker but when a claim is made or the policy checked, they discover that they are not insured, or the cover that they have paid for and thought they had is not what they have) and NFIB1G (Rental Fraud, where paying advanced fees/rent for the rental of premises which, either don't exist, are not for rent, are already rented or are rented to a multiple of victims at the same time).

We recommend a primary prevention level approach introducing awareness within specific primary and secondary school class modules that already address life skills. Given the rising fraud risks over the lifecycle, cyber-risks (including fraud) should be included in the curriculum, despite strong competition for such inclusion. The secondary prevention benefit is that this might make the group more aware of and armed against scams involving apps and the search for 'bargains'. Appropriate material will have to be researched and evaluated with children, and made available to Educational authorities for use within the curriculum. Some training will be needed but we anticipate that the existing staff will deliver the material, after consultation Teenagers need to be encouraged to assess both probabilities and consequences, and this applies to investments including crypto-markets and (even at pre-teen ages) warnings about credulous following of social media 'influencers'.

Initial Initiative 4: secondary and group/community: another initiative would be the proactive engagement of third-party institutions in targeted campaigns in specific postcodes. Banks are increasingly engaged in alerting victims to the risk of making increasing levels of payments, often overseas, in dating and other scams. While some dating websites have inadequate due diligence and validation of clients, we would suggest that in conjunction with banks and law enforcement, media and social media campaigns could be undertaken in group or community interventions through ethnic or social community groups proposed for specific NFIB categories, including: NFIB16C (Pension Liberation Fraud) for Asian or British Asian groups; financial investment scams (NFIB2B, NFIB2E) for Asian or British Asian and Black or Black British groups. These could be targeted on the basis of group and postcode, e.g., where NFIB2E is an identifiable spike in Coventry and Dudley; see also data in Table 11. Obviously, this will need careful handling with the communities, but – perhaps unlike Counter-Terrorism Prevent in some areas – this is an initiative they should be able to see is aimed at reducing their own harms and risks, not (or not just) reducing the risks some of them may pose to others.

Initial Initiative 5: secondary and group/community: a multi-agency approach to primary intervention would involve training up those working with a particular group to pass on concerns to appropriate agencies.

Part D - Developing a public health approach to frauds

Table 6has set out the sort of fraud to which the 70+ age group may be particularly vulnerable. The multi-agency initiative would involve those involved in the second initiative, but would also include training medical staff, care workers and family carers, financial institutions, and others, to identify signs of stress or distress, or unusual patterns of activity, and to know to whom to report the information, with appropriate response arrangements put in place, as always subject to resources. If nothing is done with such flows of alerts, then those providing them will stop.

The unfolding of such initiatives over a 12-month period would allow for assessments on how such arrangements may be developed in the future and then expanded: these might include, for example, targeted interventions to be undertaken for Time Shares and Holiday Club Frauds (NFIB2D) for Black or Black British ethnic groups in WS postcode, NFIB1E (Fraud Recovery) for white ethnic groups in CV and DY postcodes. We also propose wider community engagements through public meetings, involvement of community groups, local media and specialist agencies, such as the Citizens Advice Bureaux, Saga and Age Concern via targeted interventions on groups of fraud, such as investment and pensions frauds (NFIB2A, NFIB2B, NFIB6B and NFIB6C).

Initial Initiative 6: secondary and group/community: finally, we propose a specific organisational focus for secondary interventions for smaller businesses, charities and other organisations for frauds that specifically affect them, including employee fraud, procurement fraud and mandate fraud. While these are small in number, the potential losses may be high and the collateral harm – loss of employment and so on – greater. Here specialist advice and on-line or telephone hotline advice and support could be provided across a range of organisations by a trusted third party such as the Midlands Fraud Forum, who could draw on its membership for an annual portfolio of seminars and training offered as part of the WMOPCC interventions. Of course, this will need to avoid legal liability for advice given, using normal caveats.

10.5 PART D SUMMARY

The perspective we recommend takes the form of prevention-based interventions that have less to do with tackling offenders than an evidence-informed approach that, like public safety, is about the well-being and security of communities but, more like public health, is about specific aspects of that well-being as denoted by promoting ‘fraud health’. That approach will engage with community organisations and with educational health professionals but will also engage the police both for their deterrence role and, as will be discussed below, for the provision of public reassurance that their concerns are being attended to, despite economic constraints. Interventions – including coordinated interventions – will need to be considered to engage with victims, particularly if the low resource for the ‘pursue’ function continues to be shaped by existing policing priorities. (Of course, this is not an argument against increasing police resources to increase fraud disruption and justice for victims: it is an argument for a broader attack on fraud in addition to greater justice and deterrence). Though they can sometimes be counter-productive for public welfare objectives, morality and just deserts need to be taken into account when we consider the operation of public health models in the context of criminality.

Overall, we consider that a public health approach would not function effectively within the 3 Ps, especially where there is relatively little systematic information about the rationale, choice, extent, forms and balance between the Ps in determining counter-fraud interventions or their effects, particularly not on their effects on levels of ‘organised crime’ and/or on how frauds are organised. Adapting or developing many of the current initiatives within the Ps, in particular Protect, as well as some of the initiatives from overseas, would work better within a public health approach. This is for three reasons. First the approach focusses on the potential victims and their behaviour in being more aware of a range of fraud risks and carrying out due diligence before they invest, make purchases or transfer funds; second, it requires coordination between organisations and a streamlining of messages to ensure they resonate with particular groups or potentially fraudulent activities; and third, there is a credible or trustworthy source, or sources, whose role in advice, guidance and support is known and easily accessible. Elements of these can be found in existing financial institution/police initiatives on Authorised Push Payment fraud, etc., but they need to be pushed into other areas of risk.

Part D - Developing a public health approach to frauds

RECOMMENDATIONS

We will only make a limited number of recommendations to operationalise a public health approach adapted for fraud. Our starting point for a realistic public health response is that most current and future victims of fraud will not receive significant support and care (even if their case is triaged by the NFIB for dissemination to the WMP).

RECOMMENDATION 1: Central to reform is the recommendation that the WMOPCC formally takes ownership and coordination of the approach. This is necessary (a) to bring together all relevant organisations and expertise, and (b) to make strategic and financial decisions appropriate to the level and type of intervention. For any initiative based on the AF data in terms of victims' volume of fraud, median loss, age, ethnicity, repeat victimisation and postcode, the WMOPCC needs to pull together the three groupings discussed in the Report to assess current work and overlaps; appetite for engagement; initiatives elsewhere that may be applied to the WM Area; and enthusiasm for working together on a prevention strategy. 'Buy in' – both financial and in energetic support - from key stakeholders on a modest number of initiatives is needed to deliver a holistic public health approach in practice: it will evolve over time.

Without pre-empting their choices, the organisations involved should assess potential initiatives to determine levels of engagement, resources, added-value and evaluations of impacts. Given how high repeat victimisation currently is, we recommend a general focus on reducing this, which requires some prior specialist knowledge of and interest in fraud/scams, since these differ from other forms of repeat victimisation. We propose 6 possible short-medium term interventions (3 to 8 below).

RECOMMENDATION 2: for the high-volume fraud categories, we recommend a 'statement of intent' in the form of a public campaign labelled specifically as being for the WM Area involving financial services institutions, including existing information and campaigns on risk, and awareness and guidance, as well as a crafted message underlining what the police can and cannot do in the event of a fraud.

RECOMMENDATION 3: we recommend targeted tertiary interventions where repeat victims might raise their concerns – Citizens Advice Bureaux, doctors' surgeries, social care companies, community and youth groups such as Age Concern, Saga, Guides, Scouts, Youth Clubs, sports teams, and so on. These and other organisations, such as the WM Clinical Commissioning Groups (CCGs), might help ensure that ongoing mental health services are accessible for at least some victims of fraud. Conversely, such organisations should have a means to collate and coordinate identified support and supervision for vulnerable or repeat victims. Some particular vulnerabilities – for example, the increasing numbers of people with declining or severe mental capacity problems - may be given special treatment or focus. They are at risk not just from strangers but from family and friends, and even from those purporting to be professionals (such as financial advisors).

22. RECOMMENDATION 4: we recommend a primary prevention level approach incorporating fraud and financial literacy awareness within primary and secondary school class modules that already address life skills. Given the rising fraud risks over the lifecycle, cyber-risks (including fraud) should be included in the curriculum, despite strong competition for such inclusion. The secondary prevention benefit is that this might make the group more aware of and armed against scams involving apps and the search for 'bargains'. Appropriate material will have to be researched and evaluated with children, and made available to educational authorities for use within the curriculum. Some training will be needed but we anticipate that the issues will be well-known to existing staff who will deliver the material, after consultation. Such an approach should be pursued with any organisation, as we suggest above, working with young people (including Guides, Scouts, Youth Clubs, sports teams, etc); young people need to be encouraged to assess both probabilities and consequences, in a range of activities including online shopping, 'ghost broking' of motor insurance, investments such as crypto-markets and warnings about credulous following of social media 'influencers' and about lending their bank accounts for money muling.

RECOMMENDATION 5: we recommend the proactive engagement of third-party institutions in targeted campaigns in specific postcodes. Banks are increasingly engaged in alerting victims – especially those already identified as 'vulnerable' - to the risk of making increasing levels of payments, often overseas, in dating and other scams. While some dating websites have inadequate due diligence and validation of clients, we suggest that in conjunction with banks and law enforcement, media and social media campaigns could be undertaken in group or community interventions through ethnic or social community groups proposed for specific NFIB categories and/or postcodes.

RECOMMENDATION 6: a multi-agency approach to primary intervention would involve training up those working with people at higher risk to pass on concerns to appropriate agencies. The report has identified the sort of frauds to which the 70+ age group may be particularly vulnerable. The multi-agency initiative would involve those involved in the second initiative, but would also include training medical staff, care workers and family carers, financial institutions, and others to identify signs of stress or distress, or unusual patterns of activity, and to know to whom to report the information, with appropriate response arrangements put in place. This has resource implications both for those potential preventing/reporting staff and for those charged with responding to the reports.

RECOMMENDATION 7: we recommend a focus on secondary interventions for smaller businesses, charities and other organisations for frauds that specifically affect them, including employee fraud, procurement fraud and mandate fraud. While these are small in number, potential losses may be high and the collateral harm – loss of employment etc. – greater. Here specialist advice and on-line or telephone hotline advice and support could be provided across a range of organisations by a trusted third party such as the Midlands Fraud Forum, who could draw on its membership for an annual portfolio of seminars and training offered as part of the WM OPCC interventions. This might complement other efforts such as a current initiative of the Fraud Advisory Panel with SMEs.

RECOMMENDATION 8: we recommend that consideration be given to a larger (non-standing) capability for reactive investigation of large-scale frauds, alone or in combination with other forces, whether that be via the Association of PCCs, the City of London police, the National Crime Agency and the NECC, Serious Fraud Office or some future body created as a response to what is widely acknowledged as the ‘fraud policing deficit’. The public health focus should be on prevention, but preparation for corporate compliance/governance deficits on the scale of HBOS/Lloyds Reading needs to be carried out, and if there were several such large scale cases (including crypto/investment frauds) simultaneously or overlapping, it is not clear that England and Wales (let alone the West Midlands police) currently has the capacity and capability to deal with them, given the length of time they take and the resources they consume. This could fall within the original remit of the SFO, but they are not funded currently to carry out this role. We have focused in this Report on the more mundane frauds, but the public in the West Midlands and elsewhere may need reassurance that more can be done (and more quickly) with cases that are not part of ‘volume crime’ or ‘Organised Crime Groups’ as conventionally understood or as operationally classified. Of course, they may want to see more reactive response to ‘local’ frauds also, and we support up-skilling of police to deal with these among the many other areas of policing activity. Such thinking is not a conventional part of public health, but within-corporate or within-government ‘rotten pockets’ can occur in any part of the UK, and reducing the scale of harm caused by such activities is important, whether they are localised or more widely distributed geographically.

Volume I

The West Midlands Police Area Fraud Report

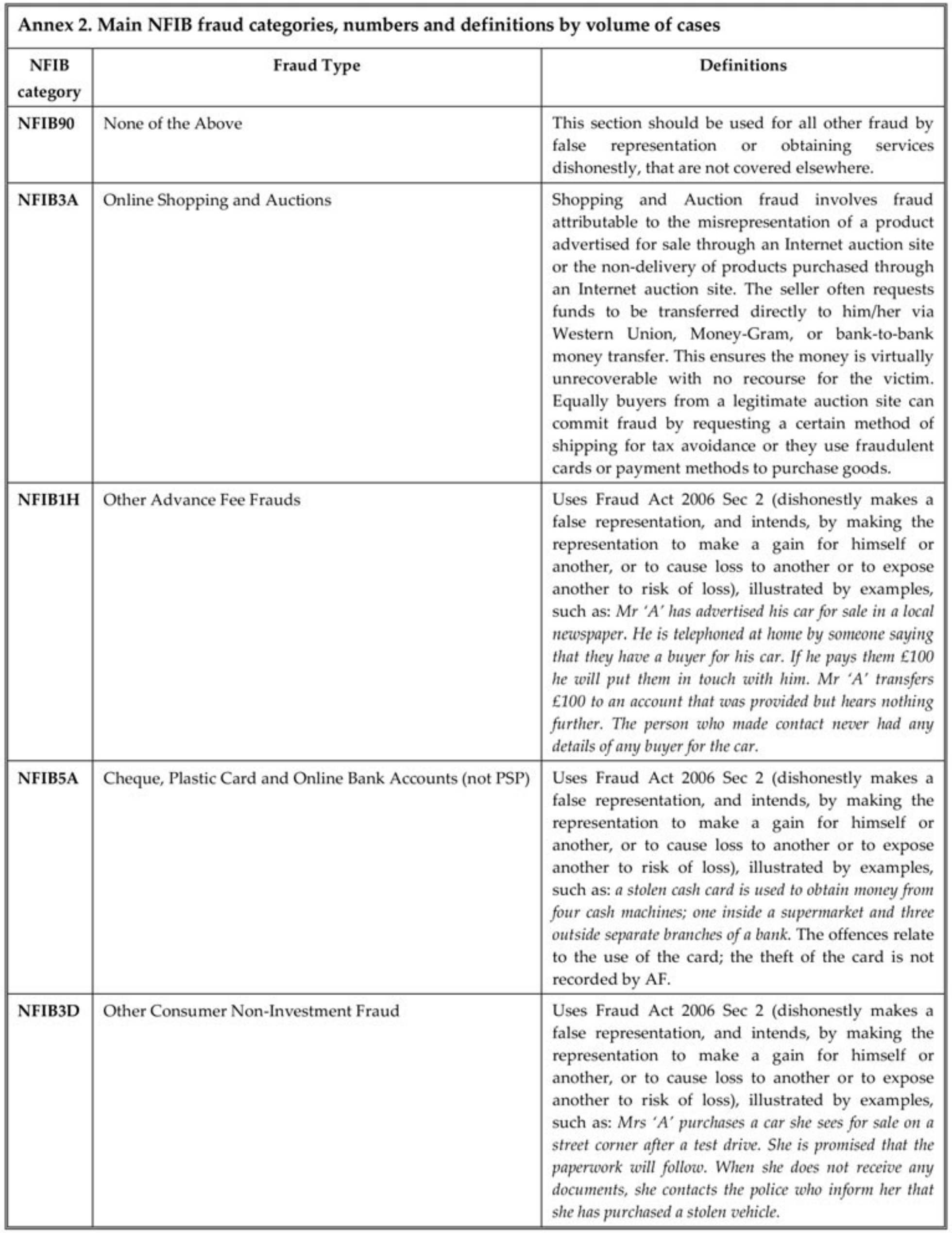
Annexes

Annexes

Annex 1. WMP Staffing and National Figures (ONS 2019: Table F1 Police officer functions (FTE), as at 31 March 2021)

	Police force/National	West Midlands	England	England and Wales
1	**Local Policing**	**3,552**	**58,930**	**62,353**
1a	Neighbourhood Policing	1,257	16,196	16,577
1b	Incident (Response) Management	1,874	36,947	39,664
1c	Specialist Community Liaison	381	4,422	4,678
1d	Local Policing Command Team	40	1,365	1,434
2	**Dealing with the Public**	**88**	**2,437**	**2,582**
2a	Front Desk	54	65	65
2b	Central Communications Unit	3	2,156	2,287
2d	Dealing with the Public Command Team	31	216	229
3	**Criminal Justice Arrangements**	**126**	**2,622**	**2,874**
3a	Custody	115	2,139	2,312
3b	Police doctors/nurses and surgeons	-	-	-
3e	Criminal Justice	3	376	437
3f	Police National Computer	-	-	-
3g	Criminal Record Bureau (now called Disclosure and Barring Service (DBS))	-	-	2
3h	Coroner Assistance	-	14	20
3i	Fixed Penalty Schemes (Central Ticket Office)	4	10	11
3j	Property Officer / Stores	-	7	9
3k	Criminal Justice Arrangements Command Team	4	76	83
4	**Road Policing**	**165**	**3,785**	**4,091**
4a	Traffic Units	162	3,557	3,850
4b	Traffic wardens / Police Community Support Officers - Traffic	-	17	17
4c	Vehicle Recovery	-	11	11
4d	Casualty Reduction Partnership	2	110	122
4e	Road policing Command Team	1	90	92
5	**Operational Support**	**439**	**7,841**	**8,281**
5a	Operational Support Team	8	348	375
5b	Air Operations	-	29	37
5c	Mounted Police	-	194	200
5d	Specialist Terrain	-	134	142
5e	Dogs Section	57	930	1,002
5f	Advanced Public Order	62	1,299	1,362
5g	Airport and Ports Policing Unit	34	756	761
5h	Firearms Unit	201	3,621	3,829
5i	Civil Contingencies and Planning	79	529	572
6	**Intelligence**	**345**	**4,604**	**4,825**
6a	Intelligence Command Team	20	194	202
6b	Intelligence Analysis / Threat Assessments	85	1,316	1,423
6c	Intelligence Gathering	240	3,094	3,200
7	**Investigations**	**1,041**	**18,838**	**19,964**
7a	Investigations Command Team	16	374	406
7b	Major Investigation Unit	326	2,936	3,014
7c	Economic Crime (including Regional Asset Recovery Team)	46	826	866
7d	Specialist Investigation Units	-	294	310
7e	Serious and Organised Crime Unit	81	2,568	2,712
7g	Local Investigation/Prisoner Processing	559	11,429	12,192
7h	Cyber Crime	13	411	465
13	**Public Protection**	**706**	**10,943**	**11,411**
13a	Witness Protection	-	516	517
13c	Protecting Vulnerable People	706	8,742	9,017
13d	Joint teams	-	1,569	1,754
13e	Public Protection Command Team and Support Overheads	-	116	123
8	**Investigative Support**	**25**	**262**	**276**
8a	Scenes of Crime Officers	11	23	24
8b	External Forensic	-	-	-
8c	Fingerprint	-	-	-
8d	Digital Forensics	-	135	135
8e	Other Forensic Services	14	96	104
8f	Investigative Support Command Team	-	9	14
9	**National Policing**	**308**	**6,326**	**6,516**
10	**Support Functions**	**199**	**6,936**	**7,415**
10a	Human Resources	8	215	223
10b	Finance	-	11	11
10c	Legal Services	-	6	6
10d	Fleet Services	-	8	8
10e	Estates / Central Building	-	9	9
10f	Information Communication Technology	-	113	147
10g	Professional Standards	39	1,098	1,160
10h	Press and Media	-	2	2
10i	Performance Review / Corporate Development	35	950	993
10j	Procurement	-	-	-
10k	Training	97	3,634	3,915
10l	Administration Support	-	243	245
10m	Force Command	11	480	515
10n	Support to Associations and Trade Unions	10	168	182
10o	Social Club Support and Force band	-	-	-
10p	Insurance / Risk Management	-	-	-
10q	Catering	-	-	-
	Other	**191**	**4,468**	**4,715**
	Total	**7,186**	**127,992**	**135,301**

Annexes



Annex 2. Main NFIB fraud categories, numbers and definitions by volume of cases

NFIB category	Fraud Type	Definitions
NFIB90	None of the Above	This section should be used for all other fraud by false representation or obtaining services dishonestly, that are not covered elsewhere.
NFIB3A	Online Shopping and Auctions	Shopping and Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. The seller often requests funds to be transferred directly to him/her via Western Union, Money-Gram, or bank-to-bank money transfer. This ensures the money is virtually unrecoverable with no recourse for the victim. Equally buyers from a legitimate auction site can commit fraud by requesting a certain method of shipping for tax avoidance or they use fraudulent cards or payment methods to purchase goods.
NFIB1H	Other Advance Fee Frauds	Uses Fraud Act 2006 Sec 2 (dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss), illustrated by examples, such as: *Mr 'A' has advertised his car for sale in a local newspaper. He is telephoned at home by someone saying that they have a buyer for his car. If he pays them £100 he will put them in touch with him. Mr 'A' transfers £100 to an account that was provided but hears nothing further. The person who made contact never had any details of any buyer for the car.*
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	Uses Fraud Act 2006 Sec 2 (dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss), illustrated by examples, such as: *a stolen cash card is used to obtain money from four cash machines; one inside a supermarket and three outside separate branches of a bank.* The offences relate to the use of the card; the theft of the card is not recorded by AF.
NFIB3D	Other Consumer Non-Investment Fraud	Uses Fraud Act 2006 Sec 2 (dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss), illustrated by examples, such as: *Mrs 'A' purchases a car she sees for sale on a street corner after a test drive. She is promised that the paperwork will follow. When she does not receive any documents, she contacts the police who inform her that she has purchased a stolen vehicle.*

Annexes

Annex 3. Period of WMP AF data: 4th May 2020 to 4th July 2021

NFIB category	Fraud Type	% of reported cases
NFIB10	False Accounting	0.01
NFIB13	Bankruptcy and Insolvency	0.03
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	0.04
NFIB15	HM Revenue and Customs Fraud	0.02
NFIB16B	Pension Fraud committed on Pensions	0.07
NFIB16C	Pension Liberation Fraud	0.12
NFIB17	Other Regulatory Fraud	0.02
NFIB19	Fraud by Abuse of Position of Trust	1.17
NFIB1A	"419" Advance Fee Fraud	0.49
NFIB1B	Lottery Scams	0.21
NFIB1C	Counterfeit cashiers' cheques	0.13
NFIB1D	Dating Scam	1.71
NFIB1E	Fraud Recovery	0.35
NFIB1F	Inheritance Fraud	0.04
NFIB1G	Rental Fraud	0.89
NFIB1H	Other Advance Fee Frauds	7.72
NFIB1J	Lender Loan Fraud	0.78
NFIB2A	Share sales or Boiler Room Fraud	1.38
NFIB2B	Pyramid or Ponzi Schemes	0.56
NFIB2D	Time Shares and Holiday Club Fraud	0.02
NFIB2E	Other Financial Investment	3.07
NFIB3A	Online Shopping and Auctions	24.06
NFIB3B	Consumer Phone Fraud	0.99
NFIB3C	Door to Door Sales and Bogus Traders	1.13
NFIB3D	Other Consumer Non Investment Fraud	6.68
NFIB3E	Computer Software Service Fraud	3.89
NFIB3F	Ticket Fraud	0.73
NFIB3G	Retail Fraud	0.41
NFIB4A	Charity Fraud	0.1
NFIB4B	Fraudulent Applications for Grants from Charities	0.01
NFIB50A	Computer Virus/Malware/Spyware	1.78
NFIB51A	Denial of Service Attack	0.02
NFIB51B	Denial of Service Attack Extortion	0
NFIB52A	Hacking - Server	0.06
NFIB52B	Hacking - Personal	1.26
NFIB52C	Hacking - Social Media and Email	3.26
NFIB52D	Hacking - PBX/Dial Through	0.01
NFIB52E	Hacking Extortion	0.54
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96
NFIB5B	Application Fraud (excluding Mortgages)	0.75
NFIB5C	Mortgage Related	0.01
NFIB5D	Mandate Fraud	0.94
NFIB5E	Dishonestly retaining a wrongful credit	0.02
NFIB6A	Insurance Related Fraud	0.06
NFIB6B	Insurance Broker Fraud	0.18
NFIB7	Telecom industry fraud (misuse of contracts)	0.08
NFIB8A	Corporate Employee Fraud	0.24
NFIB8B	Corporate Procurement Fraud	0.02
NFIB9	Business Trading Fraud	0.02
NFIB90	None of the Above	26.93

Annexes

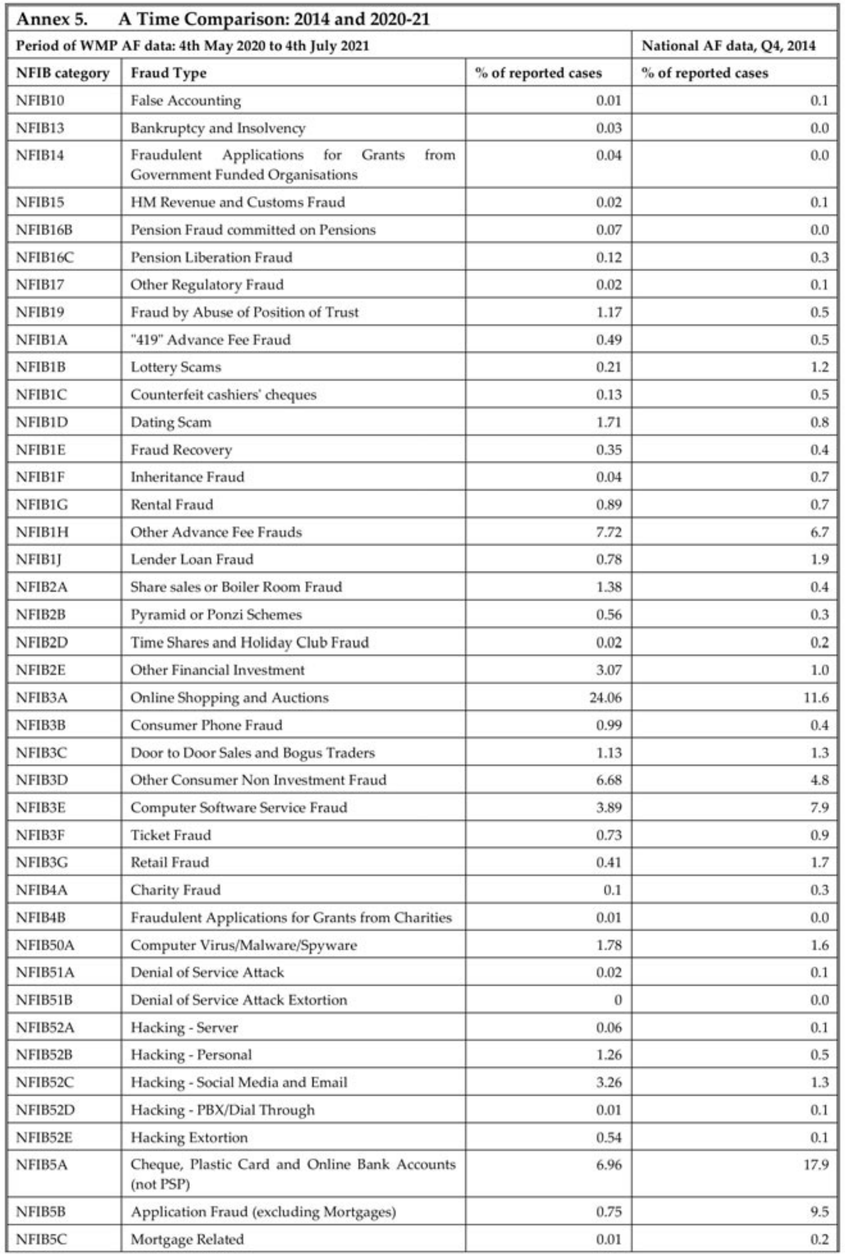
Annex 4. Repeat Victimisation by Postcode

			Repeat victim (%)					
NFIB category	**Fraud Type**	**% of reported cases**	**WMP**	**B**	**CV**	**DY**	**WS**	**WA**
NFIB10	False Accounting	0.01	50.00	100	0	0		
NFIB13	Bankruptcy and Insolvency	0.03	83.33	100	100	0	0.00	100.00
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	0.04	100.00	100	0	0		100.00
NFIB15	HM Revenue and Customs Fraud (HMRC)	0.02	100.00	100	100	100		
NFIB16B	Pension Fraud committed on Pensions	0.07	57.14	55.56	75	0		0.00
NFIB16C	Pension Liberation Fraud	0.12	32.00	33.33	50	20	0.00	66.67
NFIB17	Other Regulatory Fraud	0.02	20.00	50	0	0		0.00
NFIB19	Fraud by Abuse of Position of Trust	1.17	72.87	72	60.71	74.07	81.25	84.62
NFIB1A	"419" Advance Fee Fraud	0.49	37.50	30.77	50	45.45	66.67	33.33
NFIB1B	Lottery Scams	0.21	44.44	51.72	66.67	0	33.33	25.00
NFIB1C	Counterfeit cashiers' cheques	0.13	35.71	40	0	33.33	50.00	33.33
NFIB1D	Dating Scam	1.71	44.17	44.9	38.98	45.95	45.45	45.71
NFIB1E	Fraud Recovery	0.35	28.38	34.88	11.11	28.57	16.67	22.22
NFIB1F	Inheritance Fraud	0.04	33.33	50	0	0	0.00	0.00
NFIB1G	Rental Fraud	0.89	35.64	36.84	35.48	33.33	35.71	28.57
NFIB1H	Other Advance Fee Frauds	7.72	33.11	33.06	36.89	31.82	27.78	33.71
NFIB1J	Lender Loan Fraud	0.78	27.88	31.18	21.74	10.53	42.86	25.00
NFIB2A	Share sales or Boiler Room Fraud	1.38	41.10	44.5	35	30.77	47.62	25.93
NFIB2B	Pyramid or Ponzi Schemes	0.56	46.22	46.05	41.67	27.27	77.78	45.45
NFIB2D	Time Shares and Holiday Club Fraud	0.02	50.00	33.33	0	0	100.00	
NFIB2E	Other Financial Investment	3.07	47.38	48.66	50	38.64	38.18	50.00
NFIB3A	Online Shopping and Auctions	24.06	36.13	35.62	38.27	35.98	38.48	34.98
NFIB3B	Consumer Phone Fraud	0.99	35.24	37.78	26.32	15.38	41.18	34.62
NFIB3C	Door to Door Sales and Bogus Traders	1.13	61.92	63.97	65.79	36.36	62.50	68.42
NFIB3D	Other Consumer Non Investment Fraud	6.68	41.60	44.08	35.67	38.18	40.48	38.13
NFIB3E	Computer Software Service Fraud	3.89	40.93	42.3	35.64	35.8	44.62	41.38

Annex 4. Repeat Victimisation by Postcode

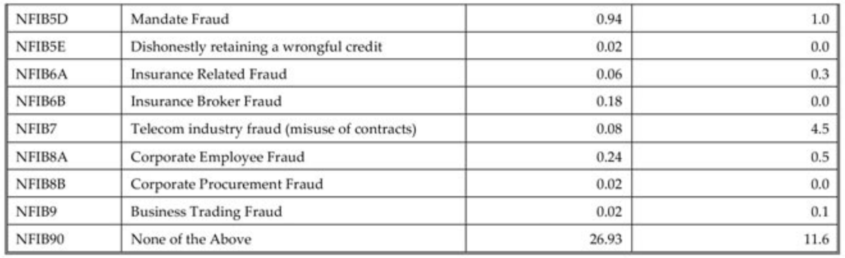
			Repeat victim (%)					
NFIB category	**Fraud Type**	**% of reported cases**	**WMP**	**B**	**CV**	**DY**	**WS**	**WA**
NFIB3F	Ticket Fraud	0.73	39.35	36.7	43.48	40	66.67	16.67
NFIB3G	Retail Fraud	0.41	76.74	78.95	55.56	100	70.00	87.50
NFIB4A	Charity Fraud	0.1	40.91	53.85	100	0	50.00	0.00
NFIB4B	Fraudulent Applications for Grants from Charities	0.01	100.00	100	0	0		100.00
NFIB50A	Computer Virus/Malware/Spyware	1.78	26.60	28.09	27.27	23.08	22.58	22.22
NFIB51A	Denial of Service Attack	0.02	75.00	100	100	0		
NFIB51B	Denial of Service Attack Extortion	0	0.00	0	0	0		
NFIB52A	Hacking - Server	0.06	91.67	90	0	100	100.00	
NFIB52B	Hacking - Personal	1.26	54.68	59.66	31.03	47.83	47.06	59.09
NFIB52C	Hacking - Social Media and Email	3.26	44.99	46.73	36	35.71	37.93	53.49
NFIB52D	Hacking - PBX/Dial Through	0.01	66.67	66.67	0	0		
NFIB52E	Hacking Extortion	0.54	34.51	43.08	18.75	20	28.57	26.67
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96	59.90	59.44	57.63	58.72	63.64	62.91
NFIB5B	Application Fraud (excluding Mortgages)	0.75	42.41	41.35	38.89	77.78	50.00	26.67
NFIB5C	Mortgage Related	0.01	33.33	33.33	0	0		
NFIB5D	Mandate Fraud	0.94	41.41	44.35	38.1	18.75	16.67	48.39
NFIB5E	Dishonestly retaining a wrongful credit	0.02	100.00	100	100	0		100.00
NFIB6A	Insurance Related Fraud	0.06	83.33	87.5	100	50		
NFIB6B	Insurance Broker Fraud	0.18	43.59	40	25	100		50.00
NFIB7	Telecom industry fraud (misuse of contracts)	0.08	31.25	50	0	0		0.00
NFIB8A	Corporate Employee Fraud	0.24	78.00	69.57	100	66.67	83.33	84.62
NFIB8B	Corporate Procurement Fraud	0.02	80.00	100	0	0		0.00
NFIB9	Business Trading Fraud	0.02	100.00	100	100	0		100.00
NFIB90	None of the Above	26.93	37.99	37.9	39.47	34.69	37.10	39.80

Annexes



Annex 5. A Time Comparison: 2014 and 2020-21			
Period of WMP AF data: 4th May 2020 to 4th July 2021			National AF data, Q4, 2014
NFIB category	Fraud Type	% of reported cases	% of reported cases
NFIB10	False Accounting	0.01	0.1
NFIB13	Bankruptcy and Insolvency	0.03	0.0
NFIB14	Fraudulent Applications for Grants from Government Funded Organisations	0.04	0.0
NFIB15	HM Revenue and Customs Fraud	0.02	0.1
NFIB16B	Pension Fraud committed on Pensions	0.07	0.0
NFIB16C	Pension Liberation Fraud	0.12	0.3
NFIB17	Other Regulatory Fraud	0.02	0.1
NFIB19	Fraud by Abuse of Position of Trust	1.17	0.5
NFIB1A	"419" Advance Fee Fraud	0.49	0.5
NFIB1B	Lottery Scams	0.21	1.2
NFIB1C	Counterfeit cashiers' cheques	0.13	0.5
NFIB1D	Dating Scam	1.71	0.8
NFIB1E	Fraud Recovery	0.35	0.4
NFIB1F	Inheritance Fraud	0.04	0.7
NFIB1G	Rental Fraud	0.89	0.7
NFIB1H	Other Advance Fee Frauds	7.72	6.7
NFIB1J	Lender Loan Fraud	0.78	1.9
NFIB2A	Share sales or Boiler Room Fraud	1.38	0.4
NFIB2B	Pyramid or Ponzi Schemes	0.56	0.3
NFIB2D	Time Shares and Holiday Club Fraud	0.02	0.2
NFIB2E	Other Financial Investment	3.07	1.0
NFIB3A	Online Shopping and Auctions	24.06	11.6
NFIB3B	Consumer Phone Fraud	0.99	0.4
NFIB3C	Door to Door Sales and Bogus Traders	1.13	1.3
NFIB3D	Other Consumer Non Investment Fraud	6.68	4.8
NFIB3E	Computer Software Service Fraud	3.89	7.9
NFIB3F	Ticket Fraud	0.73	0.9
NFIB3G	Retail Fraud	0.41	1.7
NFIB4A	Charity Fraud	0.1	0.3
NFIB4B	Fraudulent Applications for Grants from Charities	0.01	0.0
NFIB50A	Computer Virus/Malware/Spyware	1.78	1.6
NFIB51A	Denial of Service Attack	0.02	0.1
NFIB51B	Denial of Service Attack Extortion	0	0.0
NFIB52A	Hacking - Server	0.06	0.1
NFIB52B	Hacking - Personal	1.26	0.5
NFIB52C	Hacking - Social Media and Email	3.26	1.3
NFIB52D	Hacking - PBX/Dial Through	0.01	0.1
NFIB52E	Hacking Extortion	0.54	0.1
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)	6.96	17.9
NFIB5B	Application Fraud (excluding Mortgages)	0.75	9.5
NFIB5C	Mortgage Related	0.01	0.2

Annexes



NFIB5D	Mandate Fraud	0.94	1.0
NFIB5E	Dishonestly retaining a wrongful credit	0.02	0.0
NFIB6A	Insurance Related Fraud	0.06	0.3
NFIB6B	Insurance Broker Fraud	0.18	0.0
NFIB7	Telecom industry fraud (misuse of contracts)	0.08	4.5
NFIB8A	Corporate Employee Fraud	0.24	0.5
NFIB8B	Corporate Procurement Fraud	0.02	0.0
NFIB9	Business Trading Fraud	0.02	0.1
NFIB90	None of the Above	26.93	11.6