Towards a Public Health Approach to Frauds

Volume II: The Background Report

ROCU WEST MIDLANDS REGION | REGIONAL ORGANISED CRIME UNIT

MIDLANDS FRAUD FORUM

west midlands police and crime commissioner

CARDIFF UNIVERSITY | PRIFYSGOL CAERDYDD

NW260123

Volume II
The Background Report

Contents

Volume II
The Background Report

Contents

1. The research project is a two-part study into adapting or developing a public health approach to frauds. Volume I: the West Midlands Police Area Fraud Report is an empirical study of frauds in the West Midlands and how they might be responded to; and Volume II: the Background Report which provides a conceptual and contextual background using national data.

2. Volume II: the Background Report was undertaken first in order to provide our 'epidemiological' overview of frauds by (i) sketching out what a public health approach to fraud might look like and (ii) what we know (and do not know) about contemporary fraud, as an evidence base on which to set out a structured response to a range of frauds if a public health-based approach were to be developed for fraud. Much of the current work for this Background Report has been drawn from existing sources, synthesising data, perspectives and interventions. It sets out the background to and context for the more localised empirical research that is published in Volume I: the West Midlands Police Area Fraud Report.

3. A public health approach seeks to improve general health and safety by modifying underlying risk factors that increase the chance that an individual will become a victim or a perpetrator of a crime. This involves a shift towards prevention, broadly conceived. The first step is the collection and analysis of available data as an evidence base from which to assess the potential value of public health-type responses/interventions and what forms they should take.

4. Compared with the ONS-estimated scale of fraud perpetrated in England and Wales, the number of cases reported to Action Fraud (AF) is modest (less than 1 in 11 of frauds against individuals). The number disseminated by the National Fraud Intelligence Bureau (NFIB) for a police 'pursue' response is even lower. Those fraud victims – perhaps the vast majority – may be dissatisfied with the lack of visible service. The extra harm this lack of response causes is unknown. Research published in 2018 found that while there were then over three million cases against individuals each year, only 1 in 12 were reported to AF. Of those, only 27 per cent were sent out to police forces for an investigation and just three per cent ended with a judicial outcome. Although a criminal justice outcome may not always (or often) be a satisfactory outcome to them or to society at large, many victims are unlikely to receive restorative justice, harm mitigation or (depending on resource) significant assistance on reducing future fraud risks beyond general advice.

5. Especially given the impact of the pandemic on criminal court proceedings, there is no reason to expect that these judicial outcome data would have risen since 2018. Absent major changes in efficiency and skills, policing resources devoted to fraud investigation (and CPS resources) are a central constraint on improvements in this attrition process. Given the scale of frauds and limited police 'pursue' response to them, it is important to take account of the effect of both on fear of/concern about frauds, as well as the direct harms caused by frauds, and consider whether these may be better addressed through a public health approach to frauds. A response oriented to criminal investigation is not delivering what is needed/expected, but this matters because fear of crime, vulnerability, volumes of different frauds and other patterns of victimisation all might reasonably inform strategy to enhance a public health approach.

6. Notwithstanding the fairly high probability that people will become victims of fraud – around 1 in 12 people annually - 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 in the minds of the public as well as in the minds (and effective caseload) of the police. In terms of harm and engagement with victims, coordinated preventive interventions are essential. 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).

7. Given the levels of fraud, and the current mechanisms for awareness, such interventions will need to be supplemented by developing a structured, coordinated, and continuing outreach programme by trusted (and trustworthy) persons. Peer influence and community level bodies seem particularly well placed to perform this function, and it is better that such bodies proactively seek out or arrange face-to-face sessions with representative organisations – Women's Institutes, senior citizen groups, etc. - rather than rely on vulnerable or poorly-informed individuals to get safety advice from the internet. Older

people may anyway prefer leaflets and printed materials to information on the Internet alone: but the effects of different forms of advice delivery on future fraud risks need to be tested rigorously, not assumed by experts to work because their advice is right.

8. Towards a public health approach could add value to fraud responses. We consider that this 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. This will focus more on better protecting potential first time and repeat victims and seeking to build up a sense of security and resilience than on discouraging potential offenders (though there is room for research and experiments on the latter). Here, in addition to warning pop-ups and take-downs of fraudulent promotions as a supply-side approach to fraud control, a key challenge is to warn people about the dangers and try to ensure that potential victims mentally register their own situation as an example of a scam or risk about which they are aware. Awareness by itself is not enough.

9. In the light of the current epidemiology of frauds reviewed in this report, we consider that a public health approach is long overdue. We therefore make an initial analysis and assessment of fraud data relating to the West Midlands Police (WMP) Area to see how far this would help a more informed view of the added-value of such an approach and to make initial recommendations that:

   - Look behind an issue or problem to understand what is driving it;
   - Focus on prevention;
   - Propose initiatives that reflect the three levels of intervention, and are designed, delivered and tailored to be as effective as possible;
   - Propose partnerships and coordination as central because the breadth of population need requires responses (intervention) across many disciplines and services.

We consider that a public health approach offers a fresh approach to addressing a range of frauds, and one that allows the police to focus on where their competences and techniques are best deployed. However, there is currently very little evidence to demonstrate what works in preventing many types of fraud: fraud control measures rely on a weaker research base and far less rigorous experimental design to date than do many areas of general public health. An epidemiological view allows an approach to frauds that considers both the potential perpetrators and the potential victims, alongside a range of intervenors, and reduces the pressure on the police to offer a more complete suite of services than they are realistically able. Bearing in mind the issues of loss and harm we discuss in this report, exactly which interventions are best applied to what types of fraud, –– by what mechanisms, and how their effectiveness may be realistically assessed presents a data challenge and a willingness to experiment with interventions.

10. The key concerns with current status quo are:
   - Declining public confidence in the police;
   - The gaps in service for the vast 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;
   - the practical barriers to resourcing and implementing greater responses from the Criminal Justice System (CJS), including more general reforms in the disclosure requirements, international cooperation and extradition, at the kind of scale needed for fraud volumes.

11. There are many 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. These might include victim expectations, the value of personal engagement (especially in dealing with vulnerable victims who have complex needs), the links to other important local services such as Trading Standards and social safeguarding services for ‘vulnerable people’, and the need for targeted prevention which can be more readily done by local organisations who can adapt to local problems and local demographics. These might dovetail with national-led initiatives, but could be partly independent of them.

1. REPORT OVERVIEW

1.1 Research Framework

The Research project is a two-part study, published in two volumes. *Volume II: the Background Report* is conceptual and contextual, and sets the scene for the later empirical study of frauds in the West Midlands and how they might be responded to at a local and regional as well as at a national level – *Volume I: The West Midlands Police Area Fraud Report*. The conceptual and contextual study asks 3 context questions:

A. what do we know (and not know) about causes, types, levels, trends and patterns of frauds?
B. what do we know about police and other public and private sector interventions against frauds – both prevention and pursuit - and about what their effects are (including the attrition of cases from fraud identification to criminal justice)?
C. what might a public health approach to fraud look like if developed or adapted to respond to types, levels, trends and patterns of frauds?

The empirical study takes forward the questions and is intended:

1. to collect and analyse existing survey and administrative data on the epidemiology of online and offline frauds against persons and businesses within the West Midlands Police area (through Action Fraud; and also those reported fraud data that are then disseminated by the National Fraud Intelligence Bureau to the West Midlands Police for action);
2. to describe and reflect on the attrition between those experiencing fraud and police reactions to fraud; and
3. to make 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.

1.2 Volume II: the Background Report

This Report – *Volume II* – provides our 'epidemiological' overview of frauds by (i) sketching out what a public health approach to fraud (see Box 1) might look like and (ii) what do we know (and not know) about contemporary fraud that might inform a structured response to a range of frauds if a public health-based approach was progressed. Much of the current work for the Background Report has been drawn from existing sources, synthesising information, perspectives and interventions. The background study – although updated where relevant - sets the context for Volume I whose aim is to analyse the available data and envisage what it would be like to take a fresh approach to tackling fraud, treating fraud as a public health problem rather than as largely or solely a criminal justice problem. To borrow from the World Health Organisation on tackling violence, a public health approach to fraud would seek to improve the welfare of all individuals by addressing underlying risk factors that increase the likelihood that an individual will become a victim or a perpetrator of a crime. The first step in this approach is the collection and analysis of available data from a range of sources as the initial evidence base from which to consider responses/interventions.

The difference between using a public health approach and other types of crime prevention (e.g., through strategic partnerships, problem-oriented policing or situational crime prevention) is that the former aims to set out broader outcomes that may be achieved with or without policing inputs, and does not carry the same cultural baggage. But whereas public health approaches to violence may focus on interventions with offenders – stalkers and some hate crimes excepted, violence requires direct physical interaction with victims – many fraud offenders are more elusive targets for law enforcement intervention, especially given the current extremely low risks of arrest: in addition to whatever can be done with offenders, we therefore need to focus primarily on victims, potential victims, and intermediary bodies offering services through which frauds are routed. Although the overall focus of the two Volumes is on frauds in or affecting the West Midlands, its implications are national and indeed international, since we hope it will serve as a model for other areas to consider.

Box 1. What is fraud?
For the purposes of this report, we describe fraud as the loss or potential loss of income or funds – or access to data that facilitates the loss of income/funds - by individual and organisational victims, on-line and off-line, through a variety of unlawful means, including abuse of trust, deception, misappropriation, or misrepresentation. The UK Government's 2019–2022 Economic Crime Plan defines economic crime as a broad category of activity involving money, finance, or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others, including fraud against the individual, the private sector, and the public sector; terrorist financing; sanctions contravention; market abuse (encompassing the criminal offences of insider dealing, making misleading statements, and making misleading impressions); corruption and bribery; and the laundering of proceeds of all crimes.

These are not all included within the term 'fraud' for the purposes of this report, especially not terror financing or sanctions. Market abuse is the prerogative of the Financial Conduct Authority, and we will not discuss it in this report, since only its market manipulation component is fraud in our sense. Money laundering is only discussed insofar as it is relevant to the range of interventions against frauds, as a tool of proceeds of fraud restraint and confiscation, or as a mechanism through which banks, law firms et cetera, can become aware of the risks posed for the customers and clients.

1.3 Volume II: the Background Report Structure

The Sections are as follows:

- **Section 2**, in recognising that a criminal justice approach to addressing fraud is not the sole route to addressing fraud, provides a brief summary of why adapting or developing a public health approach may be considered as an appropriate framework within which to consider responses to fraud.
- **Section 3** provides a general overview of fraud and fraud statistics.
- **Section 4** assesses the effects of fraud and online fraud.
- **Section 5** addresses the impacts of fraud from individual and organisational perspectives, including impact, loss and restitution.
- **Section 6** considers how seriously the public perceive fraud and their expectations on the policing of fraud.
- **Section 7** discusses how adapting or developing a public health approach could provide an appropriate framework for potential responses.

We begin, in Section 2, with a summary of uses of a public health approach and consider if the approach may, by adaptation or development, provide a framework for addressing fraud.

2. TOWARDS A PUBLIC HEALTH APPROACH? CONSIDERING HOW A PUBLIC HEALTH APPROACH MAY BE ADAPTED OR DEVELOPED FOR FRAUD INTERVENTIONS

2.1 Why the Approach?

The aim of the first volume report – **Volume I: Towards a Public Health Approach to Frauds: The West Midlands Police Area Fraud Report** – is to envisage what it would be like to take a fresh approach to tackling fraud - treated as a public health problem rather than as largely or solely a criminal justice problem. It would, however, be a mis-characterisation to suggest that past approaches to fraud were only focused on criminal justice. The lead author of this study carried out two fraud prevention studies for the Home Office during the 1980s and one major review of the prevention of cheque and credit card fraud in 1991.

No-one has ever asserted that criminal justice is a sufficient approach to fraud, and it is taken for granted by UK policy-makers and by all police and prosecutors we have encountered that we cannot prosecute our way out of fraud (or out of any other form of 'economic crime', which includes laundering the proceeds of any crime).[1] On the other hand, the subsidiary role of criminal justice in handling 'the problem(s) of fraud' might reasonably give rise to some angst about equity in the ways our society treats different types of crime and higher socio-economic status offenders versus those who normally occupy our courts and prisons.[2]

1. Whether we can prosecute our way out of any crime is a bigger question that is out of scope here.
2. Though depending on the type of fraud, most fraudsters (by volume of frauds if not by total economic value) are not members of 'the social elite', an imprecise category. Advance fee, auction, courier and payment card fraudsters are more 'blue collar' or 'organised crime' types in terms of social background.

Harm reduction through prevention is at the core of a public health approach, as is embodied also in HMG's Serious and Organised Crime Strategy and in Violence Reduction, which differs because most violence occurs between people who know each other and/or are in predictable places. However, it should be recognised from the outset that a public health approach applied in a health context would be very different when considered for other contexts. It is an open question, for example, whether public health approaches can or should ignore wrongfulness and social legitimacy issues in focusing exclusively on harm reduction - for one important difference between health and crime is that 'crime' traditionally involves a demand for justice as well as reducing crime and making victims (and perhaps offenders) well again.[3]

Furthermore, it would be a mistake to take 'tackling fraud' as a unitary problem, since it comprises many different patterns of offender-victim-third party interaction (both national and transnational), very different scales of financial and emotional impact, and (as do nearly all crimes) different levels of 'attractiveness' to print, social and visual media coverage. Anyone reviewing contemporary news coverage would be clear that the media are deeply interested in some frauds (though they are far less interested in fraud than in murder); and in addition to its interest in celebrities and lifestyles of the rich and infamous, much of this coverage takes the form of criticising public authorities (police and non-police enforcement agencies, regulators and governments) and private bodies (banks, consumer trading websites, and social media companies) who are 'not doing enough'.[4] Part of the problem in dealing with such criticism is the incomplete understanding of how different frauds occur, and who should respond to what types of frauds, individually or collectively.

2.2 The Components of a Public Health Approach

Unsurprisingly, a public health approach is embedded in UK healthcare planning. The NHS sees the public health approach as protecting the public from threats to their health, ranging from individuals to dealing with wider factors with health impacts on segments of the public (for example an age-group, an ethnic group, a locality, or a country). The approach aims to contribute to reducing the causes of ill-health and improving people's health and wellbeing through a range of preventative measures: protecting people's health (for example from environmental or biological threats, such as food poisoning, air pollution or radiation); improving people's health (for example by helping people quit smoking, take more exercise or improving their living conditions); and ensuring that health services are accessible to all, efficient and effective (though as in much crime control policy, effectiveness is ill-defined).

The NHS Long Term Plan[5] has a strong focus on the treatment and prevention of illness by supporting patients to adopt improved healthy behaviours to help people to live longer, healthier lives, and to reduce the demand for and delays in treatment and care. The Plan focuses on specific illnesses (tobacco addiction, alcohol dependence and obesity) and service provisions to support patients to overcome the causes, particularly in areas with the highest rates of ill health. It offers two main strands:

Primary prevention means working with partners such as Government, Public Health England (and its equivalents in devolved governments) and local government to prevent disease or injury before it ever occurs through healthier choices and so reduce the risk of developing ill health, disease and premature death; and
Secondary prevention includes treatment to support the changes in behaviours or lifestyle factors that are needed to improve a person's healthy life expectancy.

The UK public health approach relies on well-established empirical datasets from which to determine trends, concerns and points of intervention, around 40,000 people already working in core public health roles (and 'core' is determined not only by required skills and knowledge but also organisational and budgetary capacity to deliver) and networks for implementation across public, private and not-for-profit sectors. Clearly, taking a public sector approach to fraud is not therefore a simple matter of transferring subject matter and levels of intervention, but it is one of conceptualising approaches to fraud that provide responses beyond those that rely solely on investigation by law enforcement. It is an approach undertaken elsewhere in the public sector, for example violence reduction.

4. It is far from clear what 'enough' would look like in the eyes of critics, but public policy needs to try to set that out.
5. See https://www.longtermplan.nhs.uk/areas-of-work/prevention/treating-and-preventing-ill-health/.

2.3 How Fraud may be Addressed Drawing on a Public Health Approach

The components noted above are concerned with prevention through awareness of/minimising risk, specific or structured interventions to promote risk reduction, and engagement with partners. The approach relies on the availability of data on which to make choices about risks and interventions, on a substantial existing staffing resource to be relocated to such work, engagement with significant stakeholders with national reach, and levers for change through policies, legislation/regulation, and allocation of resources.

One of the key stakeholders in delivering public health in the UK is local government. Its role has been driven by government policy and by legislation, but also by an awareness of where prevention was better focussed, at least in principle:

> ...the reforms also had a wider purpose, for public health teams to influence and support wider local government decisions that impact the public's health, given the strong evidence that while the NHS has a significant role to play, much of what determines health – including good-quality homes, access to stable and rewarding work, safe and secure streets and a good environment – are influenced more strongly by local government.[6]

Local government's role now extends across three levels of intervention:

- primary prevention (taking action to reduce the incidence of disease and health problems within the population, either through universal measures that reduce lifestyle risks and their causes or by targeting high-risk groups);
- secondary prevention (systematically detecting the early stages of disease and intervening before full symptoms develop – for example, prescribing statins to reduce cholesterol and taking measures to reduce high blood pressure); and
- tertiary prevention (softening the impact of an ongoing illness or injury that has lasting effects. This is done by helping people manage long-term, often-complex health problems and injuries - e.g., chronic diseases, permanent impairments - in order to improve as much as possible their ability to function, their quality of life and their life expectancy)[7].

Adapting or developing public health approach for specific crimes has been undertaken in specific areas, such as violence :

> 'like an infectious disease. It suggests that policy makers should search for a 'cure' by using scientific evidence to identify what causes violence and find interventions that work to prevent it spreading. A 'public health' approach involves multiple public and social services working together to implement early interventions to prevent people from becoming involved in violent crime'[8].

This approach has come with (limited) resources and legal requirements on coordination and cooperation:

> The Government's Serious Violence Strategy is clear that tackling serious violence is not only a law enforcement issue, it needs a multi-agency approach involving a range of partners and agencies such as education, health, social services, housing, youth and victim services with a focus on prevention and early intervention. Action should be guided by evidence of the problems and what works in tackling the root causes of violence. To do this, we must bring organisations together to share information, data and intelligence and encourage them to work in concert rather than in isolation.[9]

Some elements of collaborative working are mantras of counter-fraud policy already, but awareness of the rising levels of fraud and the limited role of law enforcement suggests that adapting or developing a public health approach may add value to addressing many forms of fraud. As the College of Policing and Public Health England[10] have pointed out:

6. Buck, D. 2020. The English local government public health reforms. An independent assessment. London: Kings Fund. p5. In our view, local government does not have a high level of control over all of these elements.
7. See Local Government Association - https://www.local.gov.uk/our-support/our-improvement-offer/care-and-health-improvement/integration-and-better-care-fund/better-care-fund/integration-resource-library/prevention.
8. https://commonslibrary.parliament.uk/how-is-the-government-implementing-a-public-health-approach-to-serious-violence/
9. Home Office. 2019. Consultation on a new legal duty to support a multi-agency approach to preventing and tackling serious violence Government response. London: Home Office. p3.
10. Public Health England and College of Policing. 2019. Public health approaches in policing. A discussion paper. London: Public Health England. For a more developed version, see https://assets.college.police.uk/s3fs-public/2021-09/policing-and-health-collaboration-landscape-review-2021.pdf

> Public health approaches start with the needs of the public or population groups rather than with individual people. This is different to healthcare where the focus is on the individual patient, or reactive policing where officers respond to calls about individual victims or perpetrators. Public health approaches involve interventions delivered at population level and targeting resources effectively through increased understanding of the population...

The components of the approach therefore include:

- Looking behind 'presenting problems' to understand what is driving them;
- Starting from the principle that prevention is better than cure (or than post-event harm mitigation);
- Skilled use and interpretation of data towards the evidence base necessary to ensure that interventions are designed, delivered and tailored to be as effective as possible;
- Developing coordinated interventions at primary, secondary and tertiary levels - Primary intervention to promote awareness of risk, generally or in relation to specific risks; secondary specific or structured interventions to mitigate or disrupt an at-risk activity; and tertiary interventions to prevent or mitigate harm and loss among repeat victims;
- Ensuring partnerships and coordination is central because the breadth of population need requires response (intervention) across many disciplines and services.

2.4 SUMMARY

Adapting or developing a public health approach seeks to improve the health and safety of many by addressing underlying risk factors that increase the likelihood that an individual will become a victim or a perpetrator of a crime. This involves shifting towards prevention, and a 'whole system' approach in developing responses.[11] The first step is the collection and analysis of available data from a variety of sources to compile an evidence base from which to assess which public health-type responses/interventions look promising or unpromising.

11. Drawn from: Police Foundation. 2019. *Public health approaches to crime prevention and the role of the police*. London: Police Foundation/KPMG.

3. COSTS, VOLUME AND RESPONSES: A FRAUD OVERVIEW

3.1 Fraud Data Issues

England and Wales currently have the best data on fraud available in the world, but that data still has some major limitations, namely the range of frauds against individuals and businesses examined in the individual and in the business crime surveys. Sometimes design flaws get embedded in systems: in an earlier analysis by some of us of 2013-14 AF data, 'other' types of frauds accounted for over 30% of incidents,[12] and this applies still to some clunky categories in Action Fraud's typologies. Scotland's most recent crime & justice survey contains a valuable section on cybercrimes, but offline fraud is not examined in it at all,[13] and extraordinarily, the Scottish Victimisation Telephone Survey 2020 – which aims to examine people's experiences and concerns about crime and safety during the pandemic, does not contain any mention of fraud, cyber or online crime,[14] apparently on the grounds that this would have taken too long and was not comparable with police recorded crime data! The Northern Ireland crime survey[15] – unlike its equivalent in the Irish Republic[16] – excluded both fraud and cybercrimes altogether, though there is now a module on cyber crime, showing that 15% of the population had been victims and 19% were attempted victims in 2019/20. Almost half the Northern Ireland population were worried about identity theft and over a quarter were worried about online banking misuse.[17]

It is defensible for different areas (and devolved governments) of the UK to be interested in and to prioritise different issues. However, apart from many frauds being ignored in Northern Ireland and Scotland, none of the three devolved government surveys – the Crime Survey for England and Wales (CSEW), the Scottish Crime and Justice Survey, and the Northern Ireland Safe Community Survey: Fraud and Cyber Crime - ask the same questions on cybercrime and fraud, making comparability across the UK impossible. Understandably, surveys exclude those lacking mental capacity, persons in institutions, et cetera, as well as (by definition) those who are not aware that they have been scammed.

This may not be a serious limitation, but these areas of vulnerability (e.g., fake Powers of Attorney, frauds against people under Court of Protection supervision) merit attention from other methodologies. What is counted, what is not counted, and what should be counted as 'risk indicators' to contribute to public health? One of the things we might learn from the Covid-19 pandemic is how conventional methods of measuring harm and initial analyses of symptoms can be mistaken and generate sub-optimal outcomes, so in this spirit, we need to consider what components of fraud are omitted from existing counts, and whether our ways of identifying them earlier as well as of handling them might be improved.

We can learn a lot from how potential victims have deflected fraud attempts. Crime surveys measure particular sorts of frauds at a point in time, and usually include only completed frauds unless they specifically include attempts. Potential fraud victims may not know about third party efforts that have protected them, so their self-reports may not be fully authoritative counts of risks or attempts anyway. Police recorded frauds are more of a flow over time than are surveys, but even in those cases in which victims or third parties make reports and these are recorded 'for intelligence' or 'for investigation', there may be significant elapsed time from the event to the reporting and recording, even disregarding the issue of the proportion of frauds that are seriously investigated or the still smaller proportion that end in a criminal justice outcome but no other outcome.[18]

12. See Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. 2015. *The Implications of Economic Cybercrime for Policing: Research report, City of London Corporation*. City of London Corporation; Technical Annex.
13. https://www.gov.scot/publications/scottish-crime-justice-survey-2019-20-main-findings/pages/13/
14. *Scottish Victimisation Telephone Survey 2020: Main Findings*, https://www.gov.scot/publications/scottish-victimisation-telephone-survey-2020-main-findings/pages/14/
15. https://www.justice-ni.gov.uk/sites/default/files/publications/justice/ni-community-safety-survey-fraud-cyber-crime.pdf.
16. https://www.cso.ie/en/releasesandpublications/ep/p-cv/crimeandvictimisation2019/personalcrime/.
17. *Cyber Crime: Findings from the 2019/20 Northern Ireland Safe Community Survey*, https://www.justice-ni.gov.uk/sites/default/files/publications/justice/cyber%20crime%20findings%20from%20the%20201920%20NISCS.PDF. The main survey asks questions about organised crime in Northern Ireland, including excise fraud, but 'mainstream' frauds do not appear in the types of crime associated with organised crime there: see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064816/Final_-_Findings_from_the_2020-21_Northern_Ireland_Safe_Community_Telephone_Survey.pdf.
18. For a very useful study of this in relation to AF (but not other sources) in 2013, see Scholes, A. 2018. The scale and drivers of attrition in reported fraud and cyber crime, Research Report 97. London: Home Office. The proportion of AF reports which had criminal justice outcomes then was 2 per cent. See also the recent reports on fraud policing by HMICFRS, examined later. Data on public prioritisation are discussed by Higgins, A. 2020. Policing and the Public: Understanding Public Priorities, Attitudes and Expectations. London: Police Foundation.

In terms of hard data – actual or identified loss – there is no central resource. While this Report discusses fraud data relating to individual and organisational victims recorded by government surveys and/or reported to the police through AF and then disseminated to the police by the NFIB (and including reporting by not-for-profit fraud prevention body Cifas and by UK Finance), the overall fraud figures usually cited exclude frauds against central government departments (e.g., benefits fraud and tax fraud), and against Trading Standards, the NHS and local government. Estimates of DWP and tax frauds are often subject to criticism by the National Audit Office and the House of Commons Public Accounts Committee.

There is thus no formal assessment of the scale of common fraud stock (fraudsters committing frauds across sectoral boundaries, police force areas or fraud categories), and thus the need for shared databases and consequential access. This has to be seen as a dynamic issue. The 'balloon theory' is commonly used in which fraud in one area that is squeezed merely reappears in another, but it is little more than an assumption or 'folk theory' supported by some anecdotes and case histories. There is no logical reason why the total stock of fraud should be constant, within the public sector as a whole, within any part of the public sector, or jointly in public and private sectors.

Further, year-on-year comparisons are 'snapshots' of fraud, rather than reflecting continuous dynamics of fraud. The unintended consequence is that the 'how much' figures do not add to some other important (and potentially difficult to answer) questions as part of a threat assessment to understand the extent to which individuals engage in a range of frauds or how far those committing fraud are sector specialists; how far the set of people and networks often labelled 'organised crime' will switch to fraud in general or particular types of fraud as a more lucrative and less risky activity than other forms of crime; how far changing attitudes in society expand or contract the potentiality for fraud among organisations' clients, customers and staff; and how far the changes in institutional cooperation and situational opportunity prevention cause fraudsters or potential fraudsters to look elsewhere to commit fraud. These all require good data on offenders, but with a low follow up to victim complaints, there will continue to be large gaps in our knowledge of offenders also, and these gaps are not readily filled.

Finally, we have noted no mechanism that gears resourcing and strategic direction on the basis of available data. As a report for the Financial Services Authority (FSA) – the predecessor to the FCA - noted, using the apparent scale of fraud losses and focussing on specific groups of perpetrators, such as organised crime, may have little value unless it also maps where the greater harms lie and how roles and responsibilities within the existing control environment map onto both losses and harms: 'the FSA needs to know which aspects of market failure leading to criminality it can effectively address (where it can make a difference). After all, knowing the scale or impact of various aspects of financial crime, but without knowing which of these the FSA can effectively address, would be unhelpful'.[19]

Nevertheless, setting aside major Serious Fraud Office (SFO)-type and tax cases which typically mature over much longer periods, the trends are clear that by volume, both frauds and concern about them are on the rise – and this is a phenomenon identified across the three relevant police jurisdictions (see Figure 1). In this study, bearing in mind our primary obligation to the West Midlands PCC, we will focus on frauds against individuals and against businesses but not against government and the public sector (even though these frauds are sometimes interconnected and committed by the same people).

3.2 The Cost of Fraud

The national fraud picture can vary across types of fraud, the threats and harms posed, the presence across sectors and between 'estimated' and 'actual' amounts. The current profile of frauds is driven by volume and estimated costs of reported cases, through crime surveys as well as reports to AF. In December 2021, the House of Commons Justice Committee announced an inquiry into the criminal justice system's

19. Dorn, N., Levi, M., Artingstall, D. and Howell, J. 2009. *FSA Scale and Impact of Financial Crime Project – Impacts of Financial Crimes and Amenability to Control by the FSA: proposed framework for generating data in a comparative manner*. London: FSA. p5.
20. https://committees.parliament.uk/committee/102/justice-committee/news/159385/new-inquiry-fraud-and-the-justice-system. In its final report – House of Commons Justice Committee 2022. *Fraud and the Justice System*. HC12. London: House of Commons - the cost was mentioned as £4.7 billion annually, a figure taken from the HMG Economic Crime Plan (see para 6).

approach to combatting fraud. Its opening statement suggested that 'fraud accounts for approximately half of all crimes committed and could cost the UK over £137 billion a year.[20] The 'could cost' is, however, interesting. We should beware of creating facts by repetition, and the larger costs figure contains a strong element of speculation.
In 2000 Home Office-commissioned report by the National Economic Research Associates (NERA) argued that discovered fraud could range from £5b–£9 billion and undiscovered fraud from £5b–£9 billion. National Fraud Authority (NFA) cost estimates rose from £30 billion in 2009 to £73 billion in 2012. The Government Counter Fraud Function (GCFF) estimates that before the COVID-19 pandemic,19F the public sector was losing between £29.3 billion and £51.8 billion a year from fraud and error, before any recoveries.[21]

Losses in the private sector vary from general estimates, such as an assessment of £45.5 billion in 2012 (of which less than £2 billion was associated with financial services), which became over £140 billion by 2017, to the administrative data issued by UK Finance which state that unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £730.4 million in 2021, and gross Authorised Push Payment fraud losses totalled £583.2 million, while banks & card companies prevented unauthorised fraud of £1.4 billion in 2021.[22] Combined losses rose from £1.2 to £1.3 billion.

The Justice Committee's £137 billion appears to be at the upper end of the estimated cost continuum, under a formula whose application of a global average loss rate to GDP would imply total losses of that much each year. The current GCFF estimate includes several unknown variables, with around £26.8 billion based on measurement of fraud and error in specific areas of income or expenditure. The rest is based on GCFF's assessment that fraud and error is likely to be in the range of 0.5% and 5% for the £503 billion where fraud and error has not been measured. That is a large range. Within this general figure, the reported losses to AF for 2019-20 and 2020-21 are presented in Table 1.

This may be compared to the pre-abolition National Fraud Authority Fraud Indicator report in 2013 which estimated fraud against UK individuals at £9.1 billion per annum, with mass-marketing fraud (£3.5 billion); identity fraud (£3.3 billion); online ticket fraud (£1.5 billion); private rental property fraud (£755 million); and pre-payment meter scams (£2.7 million) as the main types of offences. A commercial survey in 2016 stated that the cost of fraud carried out directly against individuals was £9.7 billion per year, with identity fraud being the single largest contributor at almost £5.4 billion.

Table 1. AF – reported losses

	2019-20	2020-21
Fraud	£2.3 billion	£2.35 billion
Cybercrime	£5.4 million	£9.6 million

3.3 Sources and the Volume of Fraud

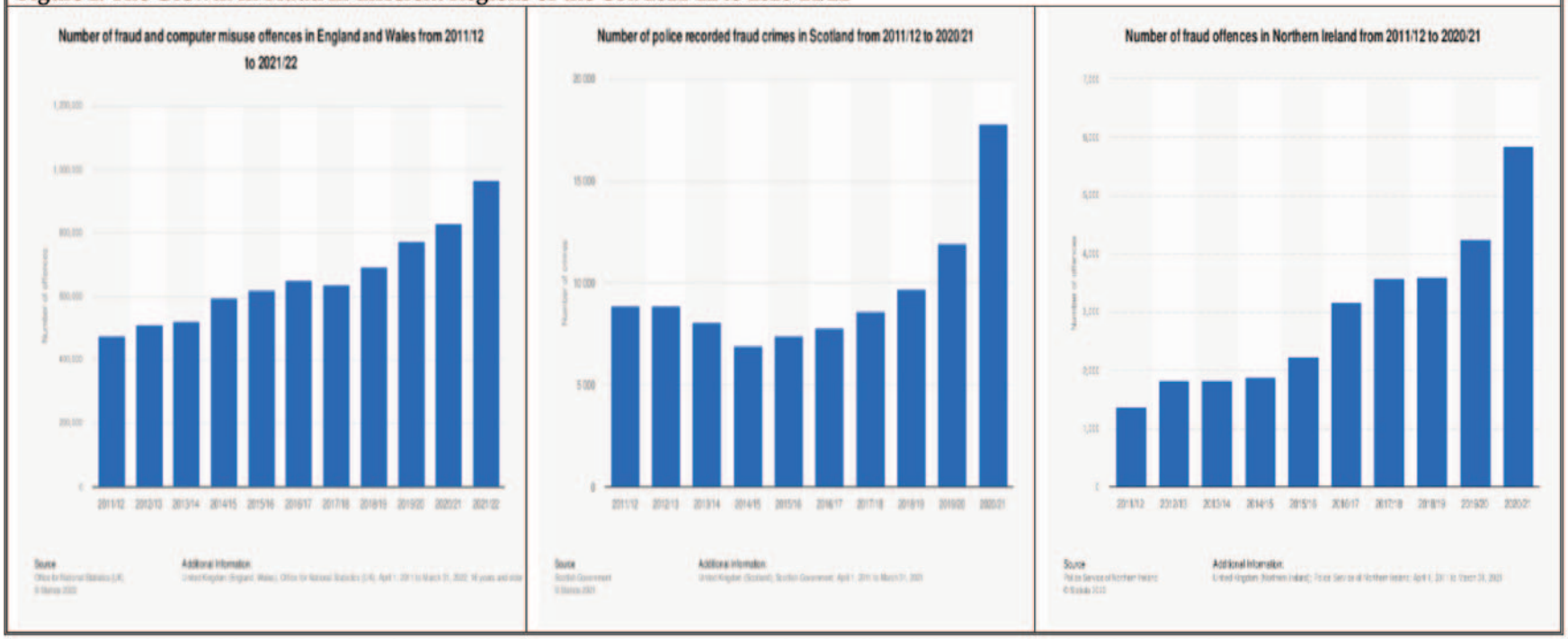
Traditionally, there are two primary sources of information about the volume of crime. The first is recorded crime data; the second, developed more in the UK than elsewhere, though still partial in its coverage, is the crime or victimisation survey. Normally, data are presented only for a geographical jurisdiction, i.e., England and Wales. But to demonstrate parallel trends, we set out the fraud trends for the UK's devolved governments in Figure 1. The levels of fraud are different, and these are not per capita data; but the direction of travel is similarly upwards in all three jurisdictions.[23]

3.3.1 Crime Survey for England and Wales (TCSEW)

Estimates from the telephone-operated Crime Survey for England and Wales (TCSEW) showed that there were 5.1 million fraud offences in the year ending September 2021 falling in the subsequent year. We set out the data below in Table 2, showing that the percentage of the population (8.9%) who were victims of fraud in that year alone was not far below the percentage who were victims of any other crime (12.3%) – if we add victims of computer misuse to the fraud data it brings it up to 12%.

21. The response to the pandemic included a number of one-off central government initiatives which focussed on speed of accessibility and payments, rather than certification and controls. As a consequence, the Department for Business, Energy & Industrial Strategy and the British Business Bank's preliminary estimates of fraud losses could be between 35% and 60% (£16 billion to £27 billion using the amount lent as at January 2021 of £44.7 billion). Similarly, HMRC's Coronavirus Job Retention Scheme, Self-employment Income Support Scheme and the 'Eat Out to Help Out' involve some £5.5 billion fraud losses (or around 8.7% of the allocated funds). This is area of dynamic estimates and responses, and figures are subject to revision.
22. UK Finance. 2022. UK Finance Annual Fraud Report, 2022. London: UK Finance.
23. At this stage we are unable to separate out the fraud from the computer misuse data for England and Wales to make them more directly comparable.

Figure 1. The Growth in Fraud in different Regions of the UK: 2011-12 to 2020-21/22



Sources: (England and Wales) ONS; Scottish Government; Police Service of Northern Ireland; Charts supplied by Statista

Table 2: Fraud and Computer Misuse Data 2020-21				
Offence group	Oct 2020 to Sep 2021 Incidence rate per 1,000 population	Oct 2020 to Sep 2021 Number of incidents (1,000s)	Oct 2020 to Sep 2021 Percentage, victims once or more	Oct 2020 to Sep 2021 Number of victims (1,000s)
ALL CSEW CRIME EXCLUDING FRAUD AND COMPUTER MISUSE	[x]	5,904	12.3	5,668
FRAUD AND COMPUTER MISUSE	151	6,982	12.0	5,517
Fraud	111	5,114	8.9	4,102
Bank and credit account fraud	61	2,838	5.0	2,294
Consumer and retail fraud	33	1,515	3.0	1,365
Advance fee fraud	10	480	1.0	441
Other fraud	6	281	0.5	214

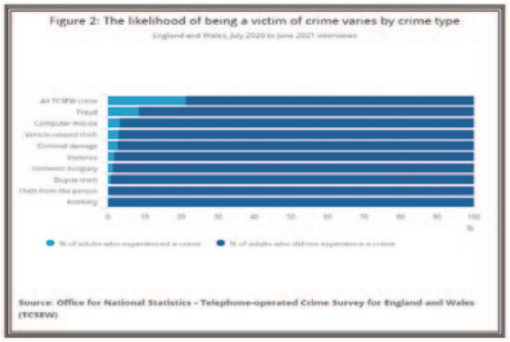
Source: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables - Appendix Table A2.

There were 5.1 million fraud offences against individuals in the year ending September 2021, a 36% increase compared with the year ending September 2019. The number of fraud victims (as contrasted with the incidents figure above) showed a significant 27% increase compared with the year ending September 2019.

The estimates included large increases in "consumer and retail fraud", "advance fee fraud" (the highest percentage increase because from a low base rate) and "other fraud" and may indicate fraudsters taking advantage of behaviour changes related to the COVID-19 pandemic, such as increased online shopping and increased savings. For example, advance fee fraud offences included scams where victims transferred funds to fraudsters via postal/courier deliveries; other fraud included investment opportunity scams.[24] A minority (26%) of these offences resulted in loss of money or property, with no or only partial reimbursement. Fraud and computer misuse offences do not follow the lockdown-related pattern of reduced victimisation, and their rises more than offset the reductions seen for other types of crime.[25]

Frauds were by some margin the most common types of crime against persons and had the highest rates of victimisation: see Figure 2. This remains the case in the subsequent 2022 updates, in which fraud had an 8% victimisation rate, and computer misuse remains the second most common offence (3% victimisation rate), though now second equal to vehicle-related theft.

3.3.2 Action Fraud and the National Fraud Intelligence Bureau



Fraud offences reported to the police are recorded and collected by the National Fraud Intelligence Bureau (NFIB) from Action Fraud and two industry bodies, Cifas and UK Finance. Action Fraud (the public-facing national fraud and cybercrime reporting centre) reported a 27% rise in fraud offences (to 413,417 offences) compared with the year ending September 2020. The data showed a 42% increase in "financial investment fraud" offences in the last year (from 15,702 to 22,372 offences) and an 18% rise in "advance fee payments" (from 43,555 to 51,407 offences). The recent volume of cases reported to AF are presented in Table 3.

Table 3. AF – reported cases						
	2019-21			2020-21		
	AF	Cifas	UK Finance	AF	Cifas	UK Finance
Fraud	326,554	363,040	132,682	413,622	318,379	143,298
Cyber-	27,187	-	-	31,322	-	-
TOTAL			849,463			9,069,44

Source: Action Fraud

24. For the most recent data, see *Crime in England and Wales: year ending March 2022*- https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022 and Nature of fraud and computer misuse in England and Wales: year ending March 2022.
25. For an excellent review of general behavioural changes from home working, see Felstead, A. 2022. Remote Working: A Research Overview. London: Routledge.

NFIB data showed referrals from Cifas (frauds against their member organisations) increased 5% (to 319,512 offences) compared with the year ending September 2020 while UK Finance reported a 49% increase (to 155,757 offences). Many cases recorded separately by UK Finance are not reported to the NFIB because they are of insufficient intelligence value. UK Finance reported a 5% increase in fraud incidents (to 3.2 million incidents) in CAMIS. There was a 53% increase in remote banking fraud (to 94,757 incidents), reflecting increases in numbers now regularly using internet, telephone and mobile banking, and the attempts by fraudsters to take advantage of this. It is not known whether there is a higher or a lower 'hit rate' as a proportion of attempted frauds, but given the low marginal cost of attempted frauds online, this may not matter to offenders so long as they obtain financial returns that satisfy them adequately.

Plausibly due in part to methodological differences, a much larger percentage (13.9%) of the Scottish than England & Wales population (5.2%) stated that they had been victims of at least one type of cyber-fraud or computer misuse 2019-20, most commonly having their device infected by a virus and having their card or bank account details stolen online.[26] These English data are not broken down at the regional level, e.g. for the West Midlands. Furthermore, these relate to the limited range of frauds measured by the ONS and Scottish surveys – card and online identity and retail frauds – and therefore are not full pictures of 'fraud'.[27]

3.3.3 The Financial Conduct Authority

Alongside data collected from regulated firms on the financial crimes (fraud, bribery and money laundering) about which the firms have knowledge,[28] a parallel large-scale UK-wide survey on financial lives – including attitudes to risk - was carried out for the Financial Conduct Authority.[29] This found that more adults have experienced potentially fraudulent activity since 2017, when the previous study was conducted. In the 12 months to February 2020:

- 2.4 million had their account or debit card used without their permission to take cash from their account or had money charged to them;
- 1.0 million had money taken from their account in some other way which involved their personal details being used without their permission;
- 2.3 million were contacted by an individual or company with a request to transfer money through their account (often known as 'money muling');
- 1.1 million were asked to share their online account log-in details, typically involving someone pretending to be their account provider;
- 1.1 million became victims of 'push payment fraud' (when fraudsters deceive consumers or individuals at a business to send them a payment under false pretences to a bank account controlled by the fraudster. The victims cannot reverse a payment even if they realise they have been conned).

Altogether, 1.9 million adults lost money to fraud in the 12 months to February 2020. Of these, 65% fully recovered their money,[30] 13% recovered some of it, 8% tried but failed to recover it, 5% did not try to recover it and 5% had not tried yet. 9.3 million (18% of all UK adults) experienced one or more unsolicited approaches about investments, pensions and retirement planning which could potentially be a scam in the 12 months to February 2020.[31] 1 million responded to an approach

26. https://www.gov.scot/publications/scottish-crime-justice-survey-2019-20-main-findings/pages/13/.
27. Fraud involves a range of organisations, sectors and types, from those handled by the Serious Fraud Office (SFO), via NCA/ROCUs, central government departments, the NHS, local police and National and local Trading Standards. Fraud may also be involved in other financial crimes; although bribery is often separated from fraud in statistics and is not highlighted separately in the *Criminal Statistics*, many company and public official bribes are also procurement frauds and involve false accounting, and since at least some of the proceeds of all crimes are laundered, there are many overlaps too with money laundering (see, for example, Lord, N., Doig, A., Levi, M., Benson, K. and van Wingerde, K. 2020. 'Implementing a Divergent Response? 'The UK Approach to Bribery in International and Domestic Contexts'. *Public Money and Management*. 40:5. pp349-359.
28. Financial Conduct Authority. 2021. *Financial Crime: analysis of firms' 2017-2020 REP-CRIM data*. London: Financial Conduct Authority, 2021.
29. Financial Conduct Authority. 2021. *Financial Lives 2020 survey: the impact of coronavirus*. London: Financial Conduct Authority.
30. Though rarely does the reimbursement from the fraudsters – intermediaries such as banks or FCA-authorised firms pay out, sometimes after civil action and usually via the code of practice, PAS 17271 - Protecting customers from financial harm as a result of fraud or financial abuse. In 2020/21 the Financial Ombudsman Service received 7,770 new complaints from fraud victims tricked into transferring money to criminals — more than double the number dealt with the previous year. It resolved 5,600 of these cases and upheld 73 per cent in favour of the customer. However, the rise has led to a backlog at the Ombudsman: One in four cases took more than 12 months to reach a final decision, while a third took between six months and a year. The survey did not ask from where the recoveries came, and asset recovery data do not differentiate.
31. This was the survey question asked, not our interpretation.

and 100,000 paid out money. By far the most common approaches involved pensions. 44% of adults stated they have had more unsolicited approaches about investments, pensions and retirement planning which could potentially be a scam from end of February-October 2020, when the survey was conducted (note that this was the earlier stage of the Covid pandemic.)

Over a third (36%) received one or more Covid-19 related unsolicited approaches which could potentially be scams. Examples include approaches designed to look like they are Government offers of Covid-19 financial support, from the NHS Test and Trace service, from TV Licensing or from HMRC. 1.4 million say they paid out money after an unsolicited approach involving Covid-19. Men were only slightly more likely than women to have been approached. 41% of those aged 18-24 said they had been a target, compared with just 28% of those aged 65+ (perhaps because of younger people's greater social media and online presence); and 40% of BAME adults had been targeted, compared with 35% of White adults (not controlling for age distribution by ethnicity).

Adults with what the FCA very broadly defined as 'characteristics of vulnerability'[32] are far more susceptible to these approaches: 12% paid out money, compared with just 1% of those with no such characteristics. Older people appear to be cagier than the young: 16% of 18-24 year olds paid out money, compared with 1% of those aged 55+. Of all who paid out some money, the average amount paid out was £6,160 and the median (half-way point) amount paid out was £240, so a small proportion of people lost considerably more than others. The FCA report does not state whether older people lost more, but this seems plausible because some of them have more money, and knowledge or beliefs about their assets could be a basis for targeting.

3.3.4 Other sources of data

Other types of survey – though using much smaller numbers and simpler sets of questions – often yield much higher rates of victimisation. A 2016 survey noted that 22% of over 55s and 32% of over 75s believe they have been targeted by an investment scam in the last 3 years, but did not examine what proportion had fallen for one of the scam attempts.[33] Since that time, scammers' techniques – e.g. in cloning websites and simulating the phone numbers of banks and police - have improved.

A representative study by Opinium for Citizens Advice found than two thirds of British adults were targeted by a scammer January- March 2021. While over 55s are most likely to be targeted, only 2% stated that they had fallen for the scam, compared with 9% of under 34s. Younger people were most likely to be targeted by text or messaging service (61%), while those over 55 were most likely to be targeted over the phone (73%). Of all those targeted by a scammer, 54% were about fake deliveries or parcels; 41% were by someone pretending to be from the government; and 12% were by someone offering a fake investment or get rich quick scheme.[34] A later representative survey by Yonder Data solutions for Citizens Advice in May 2022 asked the public if they had been contacted since the beginning of the year by anyone that they thought was trying to scam them: 77% (a substantial increase on the year before) said they had been contacted by someone that they think was trying to scam them, though only 5% of respondents said they had actually been scammed. Note that this is less than half a year's data, so the annual figures are likely to be much larger. The most common types of scams reported included:[35]

- Deliveries, postal or courier services (55%);
- Someone pretending to be from the government or HMRC (41%);
- Someone offering a fake investment or financial 'get rich quick' schemes (29%);
- Rebates and refunds (28%);
- Banking (27%);
- Online shopping (24%);
- Health or medical (13%);
- Energy scams (12%).

32. The FCA (2021: p191) defines a vulnerable consumer as someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care. Characteristics associated with four key drivers of vulnerability (poor health, low capability, low resilience or the impact of a life event) may increase the risk of a consumer's being vulnerable to harm.
33. https://www.fca.org.uk/news/press-releases/third-over-75s-targeted-investment-scams-fca-urges-consumers-take-time-check.
34. https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/36-million-brits-targeted-by-a-scammer-so-far-this-year/. The report does not give the percentage who were actually scammed.
35. https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/over-40-million-targeted-by-scammers-as-the-cost-of-living-crisis-bites/.

We can expect these proportions of attempted and successful scams to change over time. This is sufficient evidence to suggest that frauds constitute a very large and persistent national problem, even if the baggage that comes with the label of 'national security threat' may detract from appreciating the varied nature of the harms and their small individual size. Furthermore, nearly all are experienced primarily at a local level and therefore properly should be regarded as 'neighbourhood crime', though for policing and intervention purposes, multiple victims in different localities mean that they are also regional, national or international 'organised crime'.

3.4 Recorded Frauds against Individuals

Recorded crime data at a force or regional level are unintentionally made less visible to the general public (e.g. on local crime maps on https://www.police.uk/) by the fact that they are funnelled exclusively into the national reporting mechanisms of AF: it is not clear what the impact of this is, but it seems extraordinary to us that in no part of England and Wales does fraud appear on a local crime map, considering that fraud is the largest component of crime. However, the data are available nationally (and separately for the PSNI), and – to the committed investigator - they can be disaggregated at a police force level in the NFIB dashboard[36]; see Table 4. In the last 13 months to December 2021, more individuals in the West Midlands reported fraud than in any other force area apart from the Metropolitan Police.

Table 4: Fraud and computer misuse offences referred to NFIB by AF by comparable police force areas

Area Name	Number of offences	Rate per 1,000 population	% change from previous year
ENGLAND	**403,237**	**7**	**33**
Greater Manchester	17,417	6	27
West Yorkshire	14,330	6	20
West Midlands	18,777	6	31
London	98,944	11	64
City of London	18,572	[u1]	[u]
Metropolitan Police	80,372	9	39
Thames Valley	17,756	7	24

Source: Action Fraud

On the other hand, in the number of reported frauds against organisations received, West Midlands came after the City of London, the Metropolitan Police, Greater Manchester, Merseyside, Police Scotland and Thames Valley.[37] In the West Midlands area, slightly more women than men were victims and, contrary to stereotypes about 'the elderly' being the prime targets, the most common victim age groups were 20-29 and 30-39, with steadily declining victim numbers for all subsequent age groups.[38] Consumer fraud, advance fee fraud and banking fraud were the most common fraud types reported by individuals, though to avoid double-counting, many banking frauds will be taken from UK Finance data rather than police data.[39]

There are significant differences between sorts of frauds in the elapsed time from 'the fraud event(s)' (which sometimes may stretch over years) to awareness and to recognition as 'fraud' or even as 'a loss'. Most of the governmental and media attention is on relatively short term scams against individuals and banks and social security (plus pandemic loans which have taken time to crystallise), and even some of those cases side-step questions about whether victims recognise them as fraud (e.g. some romance frauds; frauds by friends, families and lawyers against vulnerable individuals; pension fund and pension liberation abuses). In fields such as violence against women, policy and practice have been informed by an understanding of the special risks posed by repeat victimisation, but despite many discussions about 'vulnerability' in policing and social work circles, this has impacted responses to fraud unevenly. In short, even in England and Wales, where much effort has been spent on improving fraud data in the period since the 2006 government costs of fraud review,[40] it can be easy to forget that 'fraud' covers a range from the kinds of large, complex cases that are sometimes taken on by the SFO – only some dimensions of which are usually 'online' - to relatively small scale single victim interpersonal offline confidence tricks.

36. A rationale for centralisation in the creation of Action Fraud was to connect up frauds against people in different geographic areas, and only some frauds against people in the West Midlands are committed against people from that region alone.
37. https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c.
38. https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c. These data do not take into account numbers in the population, which would be a better metric to use. Reported frauds may not reflect the underlying pattern of actual frauds.
39. Reporters are instructed to report to their banks or card issuers.
40. Levi, M., Burrows, J., Fleming, M. and Hopkins, M. (with the assistance of Matthews, K.). 2007. *The Nature, Extent and Economic Impact of Fraud in the UK. London: Association of Chief Police Officers*. http://www.cardiff.ac.uk/socsi/resources/ACPO%20final%20nature%20extent%20and%20economic%20impact%20of%20fraud.pdf.

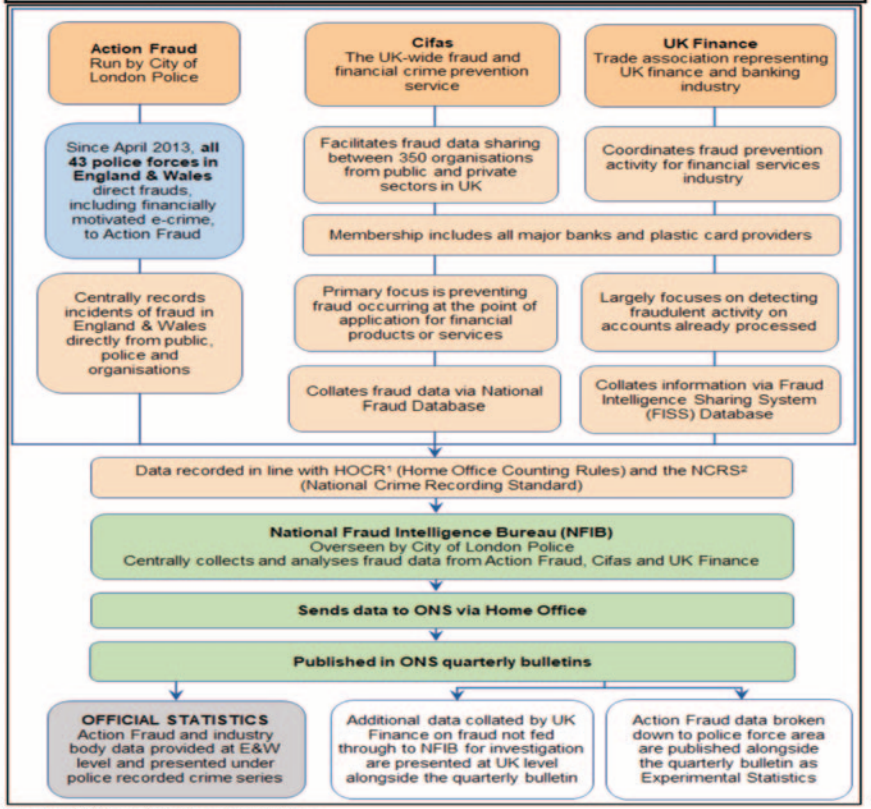
3.5 Responses and Interventions

Given the scale of fraud identified by surveys and, to a lesser extent, reports to AF, what has been the police response? There have been several potentially significant strategic, institutional and sector-specific responses to fraud, including a 2019 National Fraud Policing Strategy and a 2019 Economic Crime Plan, a 2020 Local Government Counter Fraud and Corruption Strategy, a central government functional fraud standard. Most major public agencies now have fraud units (as do banks and building societies, sometimes part of their Financial Crime Units, sometimes separate). The Economic Crime Plan is overseen by an Economic Crime Strategic Board which 'agreed that a Fraud Action Plan will be developed by the government, private sector and law enforcement and will be published following the 2021 Spending Review'.[41]

The current Fraud Action Plan (FAP) - which will be revised in 2023 - gives a central role to the National Economic Crime Centre, located with the National Crime Agency, and 2021 also saw the relaunch of the Joint Fraud Taskforce, a partnership between the private sector, government and law enforcement to tackle fraud collectively and to focus on issues that have been considered too difficult for a single organisation to manage alone. It envisages roles for the NCA and the Serious Fraud Office, and it calls for a more coordinated response across law enforcement while enhancing the roles of regional organised units. It proposes the promotion of prevention as well as investigations.

The National Fraud Policing strategy seeks to secure additional investment from government to establish nationally coordinated responses, work in partnership with the Joint Fraud Taskforce and with the finance sector to develop meaningful messaging. It also proposes that all victims who report to AF will be contacted and provided with protect advice, while local forces will embed fraud within their wider strategies and structures for identification and management of vulnerability and victim support. They will use victim data supplied by AF and Suspicious Activity Reports from regulated persons to safeguard those at risk from further harm and prevent repeat victimisation. The operational side of the policing response to fraud is shaped by the AF process, to the reports from individuals and organisations are added data from Cifas and UK Finance, and other sources, including telecommunications, government departments, and national and international police crime/intelligence systems: see Table 5.

Table 5. The Response Landscape



Source: Office of National Statistics

41. HM Government and UK Finance. 2021. *Economic Crime Plan: Statement of Progress*. London: HM Government. p6. A useful summary of current trends and issues is found in Doig, A. and Levi, M. (2021). In 2022, funding of £48.8m over three years was announced to "support the creation of a new Public Sector Fraud Authority and enhance counter-fraud work across the British Business Bank and the National Intelligence Service", half of which was to embed existing functionality. This larger area of public sector fraud is outside our brief, so we will not discuss it further.

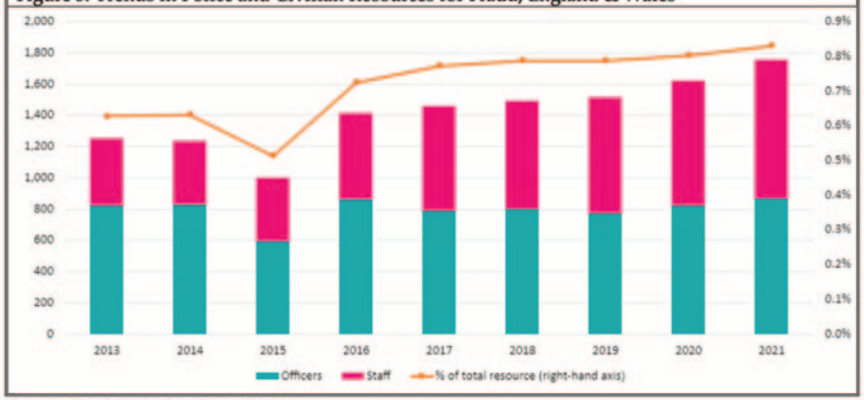
The NFIB assesses and data matches information and intelligence to identify serial offenders, organised crime groups and find emerging crime types, and then transmits these to police forces. (NFIB can also take down bank accounts, websites and phone numbers which are used by fraudsters.)

In practice, and away from the national strategic and policy statements, the reporting and investigation of fraud has been the subject of continuing concerns, none of which has been complimentary. A review commissioned following The Times' articles into the activities of AF and published in January 2020, succinctly noted that, 'for fraud to be investigated effectively, Action Fraud and the NFIB [National Fraud Intelligence Bureau] need to work seamlessly with the 43 police forces in an assured "end to end" process. However, the reality is that when cases are sent to forces for investigation, they frequently become lost among other priorities; there are disagreements about which force should take responsibility for investigations (though seldom a competition to take a case on!); and, most importantly of all, rarely are there sufficient detectives and financial investigators available to investigate them'.[42]

As of March 2021, the Home Office reported that there were 866 economic crime officers in English and Welsh forces (including regional asset recovery teams) from a total of 135,301 officers (although we note that dedicated economic crime officers are also allocated within other major crime units): this constituted 6.4% of total staff. However, our observations over decades to the present indicate that officers from economic crime units are regularly abstracted for homicide and other major enquiries, so the real proportion of fraud investigators would be lower. Using official data, the Social Market Foundation expressed the fraud policing issue as follows in Figure 3, with less than one percent of total police/civilian resource being devoted to fraud: [43]

In 2018 the Police Foundation study noted that, 'judged by conventional criminal justice outcomes the police enforcement response to fraud is poor. Just three per cent of police recorded frauds result in a

Figure 3: Trends in Police and Civilian Resources for Fraud, England & Wales



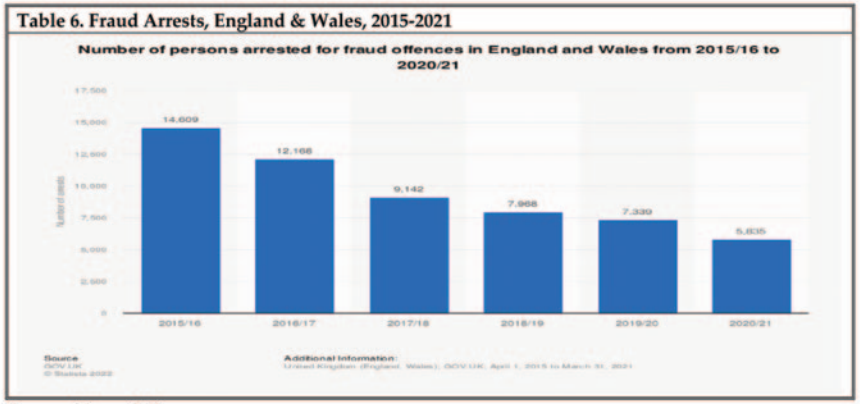
Source: Social Market Foundation

charge/summons, caution, or community resolution, compared to 13.5 per cent for crime generally. Fraud investigations also take much longer than most other criminal investigations'.[44] Historic data are unavailable for the specific case attrition, but fraud has always taken longer than other crimes for gain to investigate, despite often using information from private and third sector investigators.

In fact, the number of arrests has also been declining over the past two decades to a sixth of what they were; so as absolute numbers of survey or AF-reported frauds rise, fraud arrests have fallen in absolute terms as well as in relative terms. See Table 6 for the most recent years. We are not arguing that arrests are always the correct approach to tackling fraud, but there is little evidence of alternative approaches taken by the public sector. (June 2021-22, fraud prosecutions declined by 30 percent, the highest fall for any offence.)

42. Mackey, C and Savill, J. 2020. Fraud: A Review of the National 'Lead Force' Responsibilities of the City of London Police and the Effectiveness of Investigations in the UK. Accessible at: www.cityoflondon.gov.uk/about-the-city/about-us/Documents/action-fraud-report.pdf
43. https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/
44. Police Foundation. 2018. *More Than Just a Number: Improving the Police Response to Victims of Fraud*. London: Police Foundation. p41.

Table 6. Fraud Arrests, England & Wales, 2015-2021



Source: Home Office

Ministry of Justice data show that in the year ending June 2021, 4,406 people were sentenced for fraud, of whom a quarter (1,120) were imprisoned. The number sentenced to immediate custody has fallen over the past decade, though the percentage sentenced to custody for fraud was highest in 2020 followed by 2021, and the average length of sentence was 25 months in 2021, the highest in the decade.[45] This rise in sentencing may indicate that (perhaps excepting the small number of SFO cases) the more serious and/or 'organised' frauds are being prioritised for prosecution, though it would be unsafe to assume this without further investigation. As with much policing, cases in which there is strong evidence against local perpetrators will be the most cost-efficient to prosecute. The numbers sentenced annually from 2011-2021 are shown in Table 7.

Table 7. Annual Imprisonment Figures for Fraud, England & Wales

	2011	20112	2013	2014	2015	2016	2017	2018	2019	2020	2021	TOTAL
Fraud offences	2,841	2,828	2,559	2,438	2,305	2,238	2,162	1,875	1,529	1,540	1,120	**23,435**

Source: Ministry of Justice

Part of the issue here, as we have noted elsewhere, is that there has been a continuing shift in policing priorities and resources toward complex, sophisticated, and enduring patterns of criminal activity, which looked at fraud principally as a medium of exploitation by those already engaged in ongoing criminality and terrorism.[46] This reflected government policy but also that 'organised crime offenders' are seen by police and perhaps by broader swathes of society (though there is no social research evidence on this) as a bigger social threat than those who commit one-off or low-value frauds, or than directors, managers, staff, customers, contractors or clients of public or private sector organisations who commit fraud. Between the 'high policing' of serious or complex fraud by the Serious Fraud Office[47] and the policing of fraud committed by organised crime groups (OCGs), there is a large hinterland of fraud. This ranges from non-trivial though 'organised' - but not identified as committed by OCGs - to volume or lower-value fraud that might still cause serious distress, but which may not be dealt with by police Economic Crime Units or others within the 'Pursue' function because they simply do not have the resources to investigate them.

Overall, the process in terms of the processing, dissemination and outcomes tells its own story – see also Table 8:

- **the total number of fraud offences assigned an outcome increased** from 50,088 to 51,870 in the year ending March 2021;
- the number of **fraud offences disseminated to forces decreased** by 6% (from 26,301 to 24,805);
- an **11% fall** (down from 5,431 to 4,853) was seen in the number of disseminated fraud cases that resulted in a 'charge and or summons' (equivalent to 20% of all disseminated cases and around 1% of all recorded fraud offences).

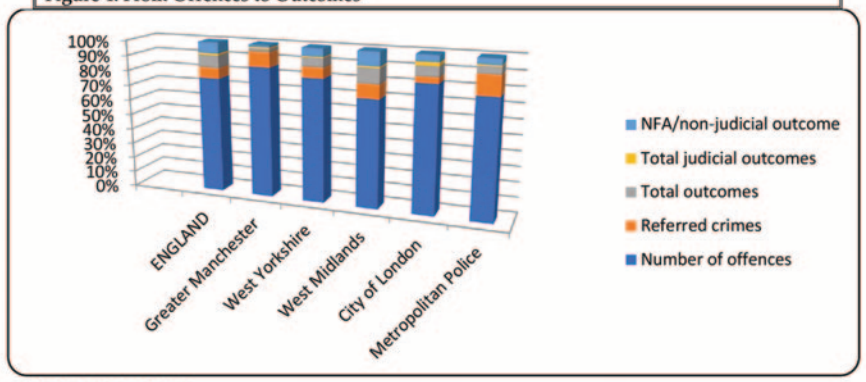
45. Tables Q 5.2 https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2021. June 2021-22, the custody rate for fraud was 32 percent, the largest rise for any offence: https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2022/criminal-justice-statistics-quarterly-june-2022-html.
46. Apart from organised crime's increasing engagement in fraud, one developing aspect of the law enforcement approach to the investigation of OCGs was pursuit of their fraud schemes or money laundering-related activity not to combat fraud as such but because it presented a significant vulnerability to investigation and/or disruption and proceeds of crime confiscation under the relevant legislation and under the broadened definition of economic crime.
47. Even before the Bribery Act 2010, the SFO increasingly focused on bribery using its Deferred Prosecution Agreements, rather than on fraud. Given the SFO's very finite resources and the NCA focus on organised crime, this inevitably left larger non-tax fraud cases to be dealt with by the police, BEIS, and regulators, if anyone at all.

Table 8. Fraud and computer misuse offences referred to NFIB by AF by comparable police force area and AF data for April 2019-March 2020							
Area Name	Number of offences	Rate per 1,000 population	% > change from previous year	Referred crimes	Total outcomes	Total judicial outcomes	NFA/non-judicial outcome
ENGLAND	403,237	7	33	36,836	44,044	5,782	38,262
Greater Manchester	17,417	6	27	1,993	443	140	303
West Yorkshire	14,330	6	20	1,221	1,054	107	947
West Midlands	18,777	6	31	2,439	2,653	234	2,419
City of London	18,572			862	1,485	500	985
Metropolitan Police	80,372	9	39	13,492	4,823	709	4,114
Thames Valley	17,756	7	24	1,177	1,345	234	1,111

Sources: Table P11, ONS and Action Fraud

Presented pictorially, it is clear that the bulk of reported fraud is not investigated fully and most frauds that receive investigative input are unlikely to be resolved through the courts; see Figure 4. A case can be made that if a fraud is unlikely to go to court, it is a waste of scarce resource to do much investigation (except for Protect or Prevent): but many might find that unpalatable.

Figure 4. From Offences to Outcomes



Source. Action Fraud

3.6 SUMMARY

Compared with the estimated scale of fraud perpetrated in England and Wales, the number of cases reported to Action Fraud is modest. The number disseminated by NFIB for a police 'pursue' response is even lower. Many victims – the vast majority – may thus feel that they received a poor service and are denied justice. Skidmore et al[48] found that while there were over three million cases against individuals each year (as measured then by an earlier CSEW), only around 260,000 (a twelfth) were reported to AF. Of those reported to AF, on average, 27 per cent are disseminated to police forces for an investigation and just three per cent ended with a judicial outcome. So although a criminal justice outcome may not always be a satisfactory outcome, many victims are falling through the cracks in the current criminal justice system and are unlikely to receive restorative justice, harm mitigation or significant assistance on reducing future victimisation.

Especially given the impact of the pandemic and justice cutbacks on criminal court proceedings, there is no reason to expect that these judicial outcome data would have risen since the Police Foundation study was published in 2018. Absent major changes in efficiency and skills, policing resources devoted to fraud investigation are a central constraint on improvements in this attrition process. Given the scale of fraud and limited police 'pursue' response, it is important to take account of the effect of both on fear of/concern about fraud, and the harm caused by fraud. These are addressed in Sections 4 and 5: both have consequences for a public health approach to fraud. Even if there had not been major cuts in policing, prosecution and courts, it is unfeasible that the Criminal Justice System (CJS) could provide an answer to such as high volume of offending, because such action is very resource-intensive and often requires good international co-operation on evidence and extradition. Whether knowledge of vulnerability might steer decisions on where to target enforcement remains an open question.

48. Skidmore, M., Goldstraw-White, J., & Gill, M. 2020. Understanding the police response to fraud: the challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management*, 40: 5. pp369-379.

4. FEARS AND CONCERNS ABOUT FRAUD

4.1 Fear of/Concern about Frauds

A public health approach could engage not only with the actual impacts of frauds but also with anxiety about frauds (both before and after they happen) and perceptions of how likely they are to happen. Anxieties and actual risks are not always well correlated, not least because of very divergent beliefs about the actual probabilities/risks as well as the effects of crime. Almost no recent studies have examined perceptions of different forms of fraud, and research has mostly focused on identity fraud, romance fraud, and payment card fraud, representing the most common types that have the readiest engagement with the public, political pressure and media. Some Australian and US studies have stressed that knowledge of scams and financial sophistication do not appear to protect against frauds, but that is different from the anxiety issue. There is also the likely fallacy that because knowledge and fear do not always or often protect against frauds, they never do so: that is an empirical question that remains largely unresearched. Prima facie, it seems very unlikely that knowledge has no effects, even if social engineering can sometimes overcome it.

Frauds and/or mis-selling of advice on re-investing company pensions may attract media coverage (which in turn helps to drive private sector, police, or regulatory prioritisation) when they happen, but they do not appear to be part of routine consciousness of fraud or even of risk. 'The public' need to be separated out into different constituencies – not just into demographics such as age, gender, ethnicity and income/wealth of individuals, but also into very small firms (almost the same as individuals), SMEs, and large businesses in different sectors. Anxieties (or lack of them) about different sorts of fraud have not been deeply explored or even voiced in the criminological or psychiatric literature, but they are tied up with perceived capacities for protection (by self and by third parties) and resilience.

4.2 Fear of/Concern about Online Fraud

As online shopping, emails and the Web/social media (inc. Instagram) as sources of believed – as contrasted with objectively credible - information have grown, attention has shifted from interpersonal or slow-time communications fraud to online fraud. To guard ourselves against risk, we need to have some expectation (accurate, reasonable or not) of the risk materialising, and when the mechanics of frauds themselves are dynamic, the Protect element in warning us and advising us about how to protect ourselves becomes trickier and may need to change over time alongside the actual Arms Race between offending and crime reduction: because of the dynamic evolving nature of the crimes, protection from scams is not a one off message like 'lock your windows and doors' or 'fasten your seatbelt'. Hence, the introduction of terms like phishing, smishing, and vishing as 'Man in the Middle Attacks' and the phone number spoofing plague: these terms help identify and differentiate the threats but also underline the need for multiple messaging by constituency, likely to be the responsibility of a range of agencies (or none!). [49]

Some of these differentiated threats have been made worse by the pandemic: stimulating or pressurising more people to bank and shop online, away from people who might have been able to advise them personally as independent third parties. Into this vacuum have come warning pop ups within most banking apps – some of which require users to sign off elecronically that they have evaluated the risks before the transaction is completed, and (though this varies between banks and opt-in/opt-out customer strategies) intentional delays in transfers of funds to new suppliers or investments, as banks try to manage the tensions between customer demands and broader expectations of guardianship against fraud risks, with additional difficulties generated by regulators' demands for higher anti-money laundering compliance. It is too early to tell what the effects are of the '159' number that potential victims can call for advice, but it is vital to appreciate that calls for advice will happen if and only if people are suspicious: suspicion and delays in compliance with the fraudster's script is a cognitive process that occurs (or often does not occur) 'in the moment'. The elapsed time from transferring funds/paying for goods and services to becoming aware that this may be fraud and then taking some action requires detailed review, and this gap is likely to change over time (and, hopefully, with better communications).

49. The Treasury Committee report has rightly drawn attention to the confusing proliferation of counter-fraud bodies, though there may be some consolidation of public sector ones in future under the Public Sector Fraud Authority (House of Commons Treasury Committee. 2022. Economic Crime. HC145. London: House of Commons).

More relevant data are available in Scotland than in England and Wales, but the evidence supports the view that cyber-fraud is far from being a marginal issue to the general public. In Scotland, in line with previous years, in 2019/20, the crimes which the public were most likely to say they were very or fairly worried about (from those asked about) were fraud-related issues. More specifically, half (50%) of Scottish adults said they were worried about someone using their credit or bank details to obtain money, goods or services, whilst 39% were worried about their identity being stolen. By comparison, under a fifth (16%) of adults were worried about being physically assaulted or attacked in the street or other public place, whilst a tenth (10%) were concerned about being sexually assaulted. Of all crimes, the crime type which adults thought they were most likely actually to experience in the next year was someone using their bank or card details to obtain money, goods or services. This echoed the pattern seen in the results on worry about crime.[50]

The Irish Republic's *Crime and Victimisation Survey 2019* asked a representative sample of adults in the Irish Republic how much they worry about being a victim of specific sorts of crime.[51] Almost a quarter (23%) of people aged 18 years and over said they worried "all the time" or "often" about being a victim of property crime, but 20% said they worried about being a victim of fraud, 20% worried about crime arising from using the internet, and 15% worried about crime which could result in physical harm or injury to them. Around half said they "don't worry at all" about crime. A fifth worried "all the time" or "often" about being a victim of fraud targeting personal finance or data, and a fifth about being a victim of crime specifically arising from their use of the internet. In each case, the figure was highest in the 45-59 age group, and in the third quintile level of deprivation. Unsurprisingly, perhaps, the proportion of people who said they "don't worry at all" about these types of crime was considerably lower among people from the most affluent areas of the country (39% for both types) than from the most disadvantaged areas (52% didn't worry about fraud, 57% didn't worry about internet use). [52] However even in the poorest areas, worry was not negligible.

4.3 SUMMARY

It is common sense that those who have more to lose and who cannot afford to replace their loss are more likely to worry about being defrauded: but rates of concern even among the less well-off are far from trivial. The fear of fraud 'normally' needs to be conceptualised as an intermittent phenomenon, for example when shopping online or answering the phone, whether landline or – more frequently nowadays - mobile, call or text, rather than as a permanent feature of the psyche about which a lot of people worry frequently.

We mostly negotiate fears about forms of crime contextually (like avoiding 'dangerous places' – however unreliable our knowledge of actual risks), though for some people in some places, fears (e.g. of domestic or stranger violence) dominate their daily thoughts. In the particular case of fraud, a phone call, a text message, or an email might be a harbinger of scams: some deal with this by not answering the landline phone at home; others mitigate it by using call-blocking technologies such as TrueCall so that only pre-installed numbers known to the householder can get through. However, there is a paradox that the form of communication might be a welcome interruption of loneliness, showing apparent friendship, or love. The denial of those opportunities (whether actual opportunities or merely hopes) is one of the unheralded and un-costed consequences of crime and/or of fear of crime.

50. Scottish Government. 2021. Crime and Justice. Edinburgh: Scottish Government. pp112-113.
51. Central Statistical Office, Government of Ireland. 2020. Crime and Victimisation Survey 2019. Dublin: Central Statistical Office.
52. For more data, see Tables 2.3 and 2.4.

5. THE IMPACT OF FRAUD

5.1 Fraud and Harm

For all the popular discussion about the impacts of fraud victimisation, as yet there is nothing in the British or US Health Surveys about it, which may reflect the conservatism of their questionnaire design. There is some literature on the mental health impact of fraud among fraud victims, especially on Elder Abuse (and particularly in the US, where it has a strong political resonance). However, as yet, there is not a specific psychiatric term for fraud phobia, and some surveys that claim to be discussing impacts of fraud refer merely to anxiety when shopping online and hesitation about new products, rather than to mental health as understood by professionals. We have not found evidence of fraud appearing in any major generic studies of mental health. Clinical psychologists we have consulted have seldom encountered fraud-related anxiety specifically, but they strongly suspect that obsessive online bank account checking would be an issue for some people. This may be attributable to fraud risks, but obsessive checking for relatively unlikely problems is a common feature of anxiety disorders - such as health anxiety (hypochondria) - and is facilitated by the easy ability to check via banking apps.

5.2 Frauds on Business

Corporate victimisation surveys have existed since the 1980s,[53] and they have been continued in various formats, mainly focused on frauds against large multinationals, and the data are broken up into national foci, partly for marketing reasons because it can be hard to tell against which country a fraud has happened.[54] The Home Office has conducted national commercial victimisation surveys this century, but has only gradually grafted on some fraud and cybercrime questions in them, though perhaps due to their conventional background in the manufacturing and retail business sectors, the financial services sector has not been included in any of them. In the 2021 Commercial Victimisation Survey (CVS), the prevalence rate for fraud showed an apparent fall from 10% in 2018 to 6% in 2021, which is in line with falls seen in fraud against financial services businesses in the same period, as reported by UK Finance and Cifas.[55] 5% of independent small retailers stated that they had experienced fraud.

The 2021 CVS showed that premises in the sector were most likely to experience retail fraud (48%) and debit or credit fraud (45%),[56] though it is common for Head Offices to handle frauds so the premises surveyed might not know that the firm had been defrauded. Fraud incidents can often have a large financial impact on businesses. The Association of Convenience Stores (ACS) Crime Report 2022 reports that the cost of fraud to convenience stores alone in 2022 was around £11 million: in the context of the sorts of figures bandied around in the fraud field, this may not sound like a large figure, but when profit margins are tight, it feels larger.[57]

In the 2021 CVS, respondents who used any computers at their premises were asked whether they had been victims of a computer misuse incident. The CVS estimated that 7% experienced computer misuse incidents, most commonly phishing/Business Email Compromise, with 5% experiencing this type of incident in 2021.[58] Fraud appeared to have a greater impact on wholesale and retail businesses than theft and crime generally, with 13% of premises reporting that fraud caused a serious or severe financial impact, 38% reporting minimal financial impact, 36% reporting moderate financial impact and the remaining 12% reporting no financial impact.[59] Respondents who said that their premise had been a victim of fraud were then asked to say how many fraud incidents out of the ten staff at their organisation reported to the police or Action Fraud.

53. Levi, M. 1988. *The Prevention of Fraud*. Crime Prevention Unit Paper 17. London: Home Office.
54. PwC's Global Economic Crime and Fraud Survey 2020: UK Findings¸ **https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2020.html** (Accessed 30 December 2021). See also the PwC 2022 survey. In the global Kroll report, only 22 percent of UK organisations responding said that fraud had had a significant impact on them: the lowest of any country in the study: see **https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2021-volume-2**.
55. **https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-year-ending-march-2021-commercial-victimisation-survey/crime-against-businesses-findings-from-the-2021-commercial-victimisation-survey.**
56. See **Table A6 - Crime against businesses: additional tables in CVS (2021).**
57. **The Crime Report 2022**, the Association of Convenience Stores (ACS); accessible at **https://www.acs.org.uk/crime-report-2022#:~:text=The%202022%20Crime%20Report%20shows,sector%20over%20the%20last%20year.**
58. See **Table H1 and H2 – Crime against businesses: headline findings from the CVS 2021.**
59. See **Table A26 - Crime against businesses: additional tables in CVS 2021**

Fewer than one in ten (8%) said that staff had reported all incidents to the police or Action Fraud, and almost half (49%) said they reported some incidents, but not all. The remaining 43% said that they had not reported any fraud incidents.

The percentage of crime incidents identified as fraud has historically varied between sectors, as in Figure 5 below. There is no reason why this variation should not happen in the future.

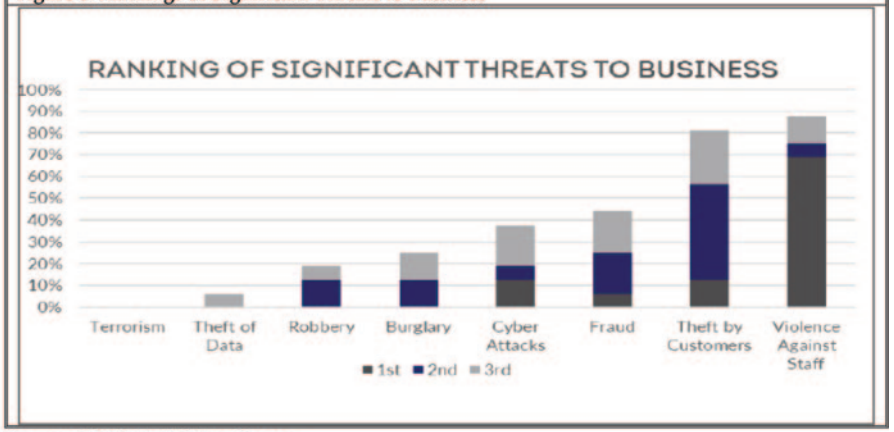
Figure 5. Fraud and Crime Incidents

Source: Home Office

The British Retail Consortium also has conducted crime surveys for many years. As with the government surveys, much depends on who is consulted when completing the survey. The 2020 Retail Crime Survey has no victimisation data about fraud, but notes that members have indicated that the two most significant areas of fraud for them are refund fraud and credit fraud, with voucher fraud also a particularly concerning area.[60] The 2021 report likewise provides no data on fraud levels but discusses areas of most significant perceived concern to business over the next three years, of which violence against staff and customer theft rank higher than fraud or cyber attacks; see Figure 6.[61]

Data breach and other surveys of SMEs as well as of larger businesses have been the province of Department of Culture Media and Sport (DCMS). The Cyber Security Breaches Survey 2022 found four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses, large businesses, and high-income charities. The most common source of threat was phishing attempts (83%). Of business victims, around one in five (21%) identified a more sophisticated attack type such as a denial of service, malware, or ransomware attack. Despite its low prevalence, organisations cited ransomware as a major threat. Within the group of organisations

Figure 6. Rankings of Significant Threats to Business



Source: 2020 Retail Crime Survey

reporting cyber attacks, 31% of businesses and 26% of charities estimate they were attacked at least once a week. One in five businesses (20%) and charities (19%) say they experienced a negative outcome as a direct consequence of a cyber attack, while one third of businesses (35%) and almost four in ten charities (38%) experienced at least one negative impact. We would add that the proper way of examining impact of fraud (and other uninsured crimes) is to ask how much business the firm would have to do to recuperate the loss. The DCMS report does not approach it in this way: looking at organisations reporting a material outcome, such as loss of money or data, gives an average estimated cost of all cyber attacks in the last 12 months of £4,200. Considering only medium and large businesses; the figure rises to £19,400.[62]

Sophisticated data on frauds against their members (as well as against the public) are available from UK Finance, Cifas, and some cyber surveys, though the sampling basis for some of the private sector studies is seldom clear. The biennial PwC Economic Crime Survey is a useful international survey of crimes against larger businesses but, like other commercial surveys, it does not ask the same questions consistently over time, and it is difficult to separate out in which countries the economic

60. British Retail Consortium. 2020. *Retail Crime Survey 2020*. London: British Retail Consortium.
61. British Retail Consortium. 2021. *Crime Survey 2021*. London: British Retail Consortium. p.24
62. Department for Digital, Culture, Media and Sport. 2022. Cyber Security Breaches Survey 2022. London: Department for Digital, Culture, Media and Sport; accessible at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

units are victims. Little methodological attention appears to have been given to those issues. Moreover, there can be ripple effects (e.g., on people in the West Midlands) if frauds impact company headquarters elsewhere, even in other countries. Other business surveys like those by KPMG and BDO map out cases dealt with by the authorities in a particular period, disregarding differences in the elapsed time from the commission of fraud to cases appearing in court.

In other cases such as insolvency abuses, the low visibility of frauds by directors against their creditors, and the disincentives to third parties such as Insolvency Practitioners to take action where they cannot identify a source of likely repayment for their fees, mean that most such abuses will never be defined, reported or recorded as fraud (by the Insolvency Service or, very occasionally, by the police or HMRC). The Financial Conduct Authority has sophisticated systems of pattern of trading recognition, but insider trading to buy or sell securities with inside information may never be picked up, especially if it the offenders are self-controlled about profit-taking: it is very seldom prosecuted.[63] Likewise, some betting frauds allied to match fixing or other offending are detectable by sophisticated data aggregation and analysis. If it was not for the industry-funded Insurance Fraud Bureau, integrating industry-wide data about car crash victims and witnesses, the awareness of and action against motor insurance frauds would be poor, but there is considerable selectivity about what is reported to the police as fraud, even to the industry-funded City of London police unit (IFED). Frauds committed by people classed as 'organised criminals' may be investigated, disrupted and prosecuted more readily than those not viewed as 'organised criminals' even if the latter are well organised enough for the frauds:[64] this has been the case since the 1960s, at least, though 'long-firm' (bankruptcy) frauds have been connected to organised crime networks since the mid-19th century.[65]

The Office of National Statistics has integrated the more reliable data from UK Finance and Cifas into its crime statistics for England and Wales, but unless cases are reported to AF, fraud statistics leave out frauds committed by or through financial and commercial institutions here and abroad against others and against individual and business customers.[66] They also omit most insolvency frauds (handled, normally non-criminally, by the Insolvency Service, whose prosecutions lead to fewer than 100 convictions per year[67]) and the sorts of consumer frauds that are dealt with by austerity-hit Trading Standards, if they are dealt with at all. Research indicated a low reporting and recording rate for possible frauds committed against people lacking mental capacity, especially if allegedly committed by friends and family. There are other cases where the attribution of a business loss to 'fraud' is disputed. It is important to stress that there is often legal ambiguity about whether commercial losses are 'fraud' or not: proving the mental element in deception and – where multiple actors are involved – who was and was not criminally responsible is deeply contested. This difficulty applies whether frauds are committed through otherwise legitimate corporations or by career offenders. Trading Standards often use strict liability legislation to prosecute and have high conviction rates.

5.3 The Impacts on Victims

Research for the Victims Commissioner segments victims according to their level of vulnerability (for example, whether they were a repeat victim), risk factors relating to the incident (whether the victim engaged in behaviour that may make them more vulnerable to fraud – in our view, a contentious category), risk factors relating to the victim themselves (age, for example), and the self-declared harm caused by the fraud. Victims are mapped across three broad categories: 'high-vulnerability victims' (representing 22% of all fraud victims), 'medium-vulnerability victims' (23%), and 'low-vulnerability victims' (55%). The analysis suggests there were around 700,000 high-vulnerability victims in 2018/19. Within the

63. Prosecutions for insider trading in recent years are extremely rare – see A. Ellson 'Only two insider traders caught by City watchdog in half a decade', *The Times*, 13 June 2022. Opinions might reasonably vary about what priority should be given to insider trading compared with other forms of financial misconduct supervised by the FCA.
64. This is implicit in the reactions to covid-19 pandemic loans frauds.
65. See Levi, M. 2008 *The Phantom Capitalists*. London: Routledge.
66. See, for example, the ongoing controversy over the then HBOS Reading 'rogue unit' frauds, which has rumbled on to the present over deeply contested compensation issues. The fraud, which took place before Lloyds rescued HBOS in 2009, damaged about 200 businesses. It involved HBOS bankers and consultants who exploited reckless credit policies to steal hundreds of millions of pounds from the bank and from business customers. Six people were jailed in 2017. It has been reported that an offer of £3 million each has been made to the victims (*The Times*, 14 June 2022).
67. https://www.gov.uk/government/statistics/insolvency-service-enforcement-outcomes-monthly-data-tables-202122 (accessed 2 February 2022).

'high- vulnerability' cluster (22%), victims were likely to have experienced financial loss, with property or money taken, and were likely to say they had been affected a lot and to have experienced severe or multiple emotional reactions, including anxiety or depression. However, over half of fraud victims fell into the 'low-vulnerability' category (55%), equating to about 1.74 million people. This might suggest that although the overall scale of fraud is very large, more than half of its victims may need little support and that the very limited resources for victim support should be targeted elsewhere.[68] The need for support may not relate to the amount of money lost: some groups of victims are unlikely to need emotional support even if they have lost a lot of money, while others may need help even though they did not lose money, or their loss was reimbursed.

Economists working with Which? researchers have explored the evidence on the relationship between fraud and subjective wellbeing.[69] Using more than 17,000 responses to the CSEW between 2017 and 2020, being a scam victim is associated with significantly lower levels of life satisfaction, lower levels of happiness and higher levels of anxiety. It is also associated with people self-reporting worse general health. Using an approach in HM Treasury's guidance on wellbeing analysis, they estimated that this lower level of life satisfaction (-0.17 on a scale of 0-10) is equivalent to an average £2,509 per victim. The negative wellbeing impact of online fraud is higher at £3,684, but the difference between online and offline is not statistically significant. These average wellbeing (or perhaps 'ill-being') harms for victims far exceed the average financial loss of £600: "with 3.7 million incidents of fraud experienced in 2019-20, we estimate that the total losses in wellbeing associated with fraud victimisation amount to £9.3 billion per year" (p.5). The losses in life satisfaction associated with being a fraud victim are comparable with those associated with being threatened or being a victim of theft. Around three quarters of fraud victims in England and Wales are affected emotionally by the experience, and 8% are 'very much' affected.[70] Given the numbers scammed, this is a lot of victims who potentially might want help, and providing help to all harmed victims is challenging.

5.4 Recovery and Compensation

5.4.1 Introduction

Overall, 1.9 million UK adults lost money to fraud in the 12 months to February 2020, before the Covid-19 pandemic.[71] Of these, 65% fully recovered it, 13% recovered some of it, 8% tried but failed to recover it, 5% did not try to recover it and 5% had not tried yet. Prosecution data are not broken down by area, so it is not possible to set out how patterns of prosecution mapped against the losses. Despite the banks' protocol (see 5.4.3 below; the 2019 Contingent Reimbursement Model Code and currently under review by the regulator[72]), compensation for victims of push payment fraud remains a contested space, with allegations that some banks are insufficiently tolerant of customer foolishness appearing regularly in the press, though many readers' comments on those press articles counter that the banks should not be responsible for customer foolishness. However, though it is a well-publicised issue (see reports in Money Which) and a source of much anxiety, this compensation issue represents only a modest percentage of total fraud losses. Some discussions conflate authorised and unauthorised losses. The UK Finance figures for 2021 show:[73]

- Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £730.4 million in 2021, a decrease of seven per cent by value compared to 2020.

68. Poppleton, S., K. Lymperopoulou, and J. Molina, *Who suffers fraud? Understanding the fraud victim landscape*, Victims Commissioner, 2021.
69. Which and Simetrica-Jacobs. 2021. *Scams and Subjective wellbeing: Evidence from the Crime Survey for England and Wales* London: Which?. Eales
70. *Nature of fraud and computer misuse in England and Wales: year ending March 2019*, ONS, 2020. It is a finding replicated in the EU where around 8 in 10 consumers who experienced some kind of scam in the last two years felt emotional or physical harm as a result, rising to around 95% among those who had suffered a financial loss (see European Commission. 2020. *Survey on "Scams and Fraud Experienced by Consumers"*. Final Report. Brussels: European Commission).
71. Financial Conduct Authority. 2021. *Financial Lives 2020 survey: the impact of coronavirus*, London: Financial Conduct Authority. We would add that more may have lost money to fraud but were not aware of it, and some may have misattributed licit losses to fraud.
72. See **https://www.psr.org.uk/our-work/app-scams/.**
73. **https://www.ukfinance.org.uk/news-and-insight/press-release/cross-sector-action-needed-criminal-gangs-steal-billions**. See also *Annual Fraud Report 2022*, **https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022**

- Authorised fraud losses: In 2021, criminals impersonated a range of organisations such as the NHS, banks, police and government departments via phone calls, text messages, emails, fake websites and social media posts to trick people into handing over their personal and financial information. They subsequently used this information to convince people into authorising a payment.
- There were 195,996 incidents of APP scams in 2021 with gross losses of £583.2 million – an increase of 39% by value on 2020 - including:
  - £214.8 million lost to impersonation scams: the largest category of APP losses.
  - £171.7 million lost to investment scams, the second largest category of APP losses.
  - £64.1 million lost to 99,733 cases of purchase scams, the most common type of scam – accounting for 51 per cent of all cases.
- A total of £271.2 million were returned to victims of APP scams, accounting for 47 per cent of losses. A slightly higher percentage (51%) were returned after being assessed under the APP voluntary code. This compensation rate continues to be a contested space.

Though Google, TikTok and Amazon – to be followed by Meta and Microsoft -have subsequently taken some measures to check advertisers' claims that they are authorised by the FCA, a significant proportion of unauthorised losses are attributable to advertisements and (increasingly) social media on Google, Amazon, eBay and Facebook/Instagram (now Meta), who also may have played some role in part in the £583.2m. It may be deduced that with the exception of Invoice/Mandate, there are often multiple payments; that there is higher probability of being refunded if one is a victim of Bank/Police Impersonation, Advance Fee or CEO Fraud; that Purchase APPs are the most common by volume (but have the lowest average loss); and only Investment, Invoice/Mandate and CEO frauds involve average losses of greater than £10,000. Between 2019 and 2021, the FCA paid at least £1,179,336 to online companies to warn about scams and on other campaigns.[74] So though Google and some other firms are now exercising more diligence, the advertisers got paid both by the scammers and by the FCA. (The Online Safety Bill 2022 – scheduled to return to Parliament - may deal with this issue, at least as regards legal responsibility: but the rate and speed of take-downs of scams remains an important operational and public welfare issue.)

5.4.2 Recovery

In addition to compensation to individuals from banks, and civil lawsuits in which the victims are plaintiffs (for which important component there are no data available), experimental statistics on Civil Recovery Order receipts covering the financial years from 2016 to 2017 until 2020 to 2021 are now available, alongside the proceeds of crime recovered through International Asset Recovery.[75] £355 million was recovered in the total proceeds of crime (including fraud) from Confiscation Orders, Forfeiture Orders and Civil Recovery Orders receipts in the financial year 2020 to 2022 (see Figure 7); a substantial increase from previous years, due to the increase in the proceeds recovered from Confiscation and Forfeiture Order receipts.

Court-ordered compensation is a very modest proportion of total losses from fraud, and confiscation orders made and enforced constitute a tiny proportion of the estimated proceeds of crime. Some of this gap is met from civil fraud and other litigation, but at this moment, data are unavailable, and unless there is litigation support from third party funders, victims would need considerable means to undertake such action, not least because they have to be able to show that they can pay the defendant's costs if they lose. The distribution of losses in the AF data make it plain that few of these would be the sorts of victims who would pursue civil remedies or have cases taken on by private prosecutions. (Some 'rogue trading' victims in Trading Standards cases might collect from Small Claims Courts, et cetera: but these are hard to pursue: some local Trading Standards, e.g., Dudley in the West Midlands, have an active prosecution policy and very high conviction rate in cases where rogue traders refuse to compensate after receiving warning letters.)

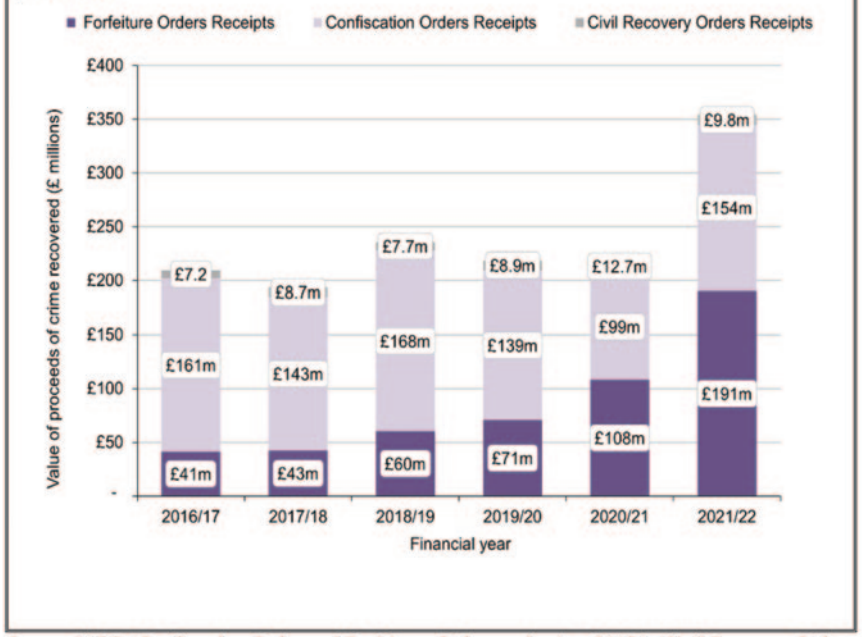
5.4.3 Compensation for fraud victims: current practice

Fraud victims can in principle be compensated in several ways: from court orders following public or private prosecutions and criminal

74. House of Commons Treasury Committee. 2022. Economic Crime. HC145. London: House of Commons. p29.
75. https://www.gov.uk/government/statistics/asset-recovery-statistical-bulletin-financial-years-ending-2016-to-2021/asset-recovery-statistical-bulletin-financial-years-ending-2016-to-2021.

conviction (including confiscations under the Proceeds of Crime Act 2002, where compensation should be paid out of confiscated funds); from compensation schemes for losers in 'failed' regulator-authorised investments and company pension schemes; from civil litigation, including that supported by litigation finance firms in return for a percentage of the costs awarded; and from industry schemes such as the Contingent Reimbursement Model Code 2019 bank agreement to compensate fraud victims.

Figure 7. The value of proceeds of crime recovered from Confiscation Orders, Forfeiture Orders and Civil Recovery Orders receipts from financial year 2015 to 2016 until financial year 2021 to 2022 in England and Wales, Northern Ireland jurisdictions and those which have no recorded jurisdiction



Source: JARD (Confiscation Order and Forfeiture Order receipts) and NCA (Civil Recovery Order receipts)

This (currently voluntary) code states that customers need to have a 'reasonable basis' for believing the payee is whom they expect. Customers may have to explain why they believed the person they were paying was legitimate, an issue that has been eased somewhat by the widespread but not yet universal adoption of Confirmation of Payee in e-banking, showing the name of the payee to the person wanting to send funds. The code also states that banks must provide customers with 'effective warnings' when they are making an unusual payment - such as when they are paying someone new. This is often done via banking apps which force some warnings for new payees. It is advantageous for compensation if consumers tell their bank that they are vulnerable, because the banks are obliged to take extra measures to protect vulnerable customers, and 'vulnerability' is not an obvious condition.

There has been a sharp rise in authorised push payment (APP) fraud, where people are tricked into sending their money to accounts controlled by criminals; see Figure 8. Though prevention efforts reduced the rate by 17% in the first half of 2022, in 2021, the number of APP fraud cases was vastly more than that recorded in 2019, and costs totalled 39% more than in 2020. Most high street banks - Barclays, HSBC, Santander, Co-op, Lloyds, Metro, Starling, National Westminster Bank and Virgin Money - are already signatories to the Contingent Reimbursement Model Code set up in May 2019 to combat fraud. This has improved refund rates for victims, supplemented by press stories that pressurise banks into 'doing the right thing'. TSB has offered customers a fraud refund guarantee since April 2019. However, the code has been inconsistently applied by different banks and the average reimbursement rate remains at less than 50 per cent since its introduction.[76]

Figure 8. APP fraud increase

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	145,207	188,964	30%	9,407	7,032	-25%	154,614	195,996	27%
Payments	228,946	333,751	46%	15,625	11,386	-27%	244,571	345,137	41%
Value	£347.4m	£505.9m	46%	£73.3m	£77.4m	5%	£420.7m	£583.2m	39%
Returned to Victim	£163.4m	£246.8m	51%	£27.4m	£24.4m	-11%	£190.8m	£271.2m	42%

Source: UK Finance (2022)

Fraud victims who disagree with their bank's decision can appeal to the Financial Ombudsman Service (FOS) which has been inundated with claims: 73 per cent – over twice the rate in other FOS sectors - of disputed bank fraud cases are found in the customers' favour. The Payment Systems Regulator stated that banks could do more to help

76. See https://service.betterregulation.com/document/389049.

those defrauded of their savings: "it is unlikely that victims have not acted appropriately in 50 per cent of cases."[77] There remain many arguments over the extent of the duties of banks towards their customers and pending definitive legal rulings, we anticipate that these will continue, fuelled by the unpopularity of banks and tensions between that and expectations of care and prudence on the part of those paying away their money in ways that afterwards are shown to be unwise.[78]

Much of the media coverage has been about deficiencies in repayment of fraud victims by banks and, to a lesser extent, the FCA (in disputes over whether the scheme applies, as well as over alleged dilatoriness in intervention).[79] In the latter sort of case, the allegation is one of fraud or rip-off of customers by authorised financial services firms. One of the more heavily covered examples was the fraud by a staff group at HBOS Reading against business customers. Victims may or may not care whether their compensation comes from offenders or some intermediary firm who have been negligent or from a formal compensation scheme: there is no evidence about victim views on this.

The Sentencing Council for England and Wales notes that a court must consider making a compensation order in any case where personal injury, loss or damage has resulted from the offence. It can either be an ancillary order, or a sentence in its own right. The court must give reasons if it decides not to order compensation (Sentencing Code, s.55). Though the Council's primary focus is on violent crime, the court should consider two types of loss:

- financial loss sustained as a result of the offence such as the cost of repairing damage or, in case of injury, any loss of earnings or medical expenses;
- pain and suffering caused by the injury (including terror, shock or distress) and any loss of facility. This should be assessed in light of all factors that appear to the court to be relevant, including any medical evidence, the victim's age and personal circumstances.

However, compensation orders require conviction, and as we have noted elsewhere, the number of offenders arrested for and convicted of fraud is modest and falling absolutely and as a percentage of fraud. It also requires payment out of the realisable assets of those convicted, and many offenders 'offend to spend', quite apart from any gaps in financial investigators' knowledge of where assets are.[80] The longer the elapsed time post-offending, the less the chances of any significant compensation being ordered and paid.

The number of compensation orders for all offences in England and Wales in 2021 were as follows: indictable-only, 6; triable either way, 1,718; summary non-motoring, 2,494. In the year ending June 2021, compensation orders were imposed on 60 people for fraud (the highest in the previous decade was 148 in 2013) – 1.36% of those convicted – so it is plainly not a frequent occurrence![81] Data on sums awarded are not available.

A very small subset of compensation cases relates to the work of the Serious Fraud Office. In the year ending March 2021, 5 individuals were sentenced. In addition to £47.4m in fines, penalties and costs from (corporate) Deferred Prosecution Agreements, 8 financial orders were obtained to a value of £7.4 million, and over £220,000 was paid in compensation for victims,[82] collected from Orders made in previous financial years. The SFO will seek Compensation Orders where there are victims: no Compensation Orders were sought during 2020-21 as there

77. https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/; and 'Banks to be forced to offer scam victims compensation', James Pickford, *Financial Times*, Nov 18 2021; (accessed 2 January 2022). The government has stated that it will give the PSR the power to require all banks to comply consistently and to publish bank reimbursement rates. See the 2022 consultation https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/.
78. For a High Court ruling on victims' limited rights against their bank, see Philipp v Barclays [2021] EWHC 10 (Comm), which affirmed the previous case law Barclays Bank plc v Quincecare Ltd [1992] 4 All ER 363. Mrs Philipp was asked by the Bank when making the transactions whether she wished to proceed, and confirmed that she did. She also confirmed to the Bank (incorrectly, but as directed by the fraudster) that Dr Philipp had had prior dealings with one of the purported beneficiaries of the transactions. Mrs and Dr Philipps also refused to engage with police enquiries, having been told by the fraudster that police involvement could jeopardise the FCA/NCA investigation. The judge ruled that the Bank had no legal obligation to prevent the APP fraud beyond the efforts it had shown in this case.
79. https://mouseinthecourtroom.wordpress.com/2022/06/21/did-internal-politics-and-a-culture-of-confusion-at-the-fca-fail-p2p-consumers/
80. Levi, M. 'Reflections on Proceeds of Crime: A New Code for Confiscation?', in Child, J. and Duff, A. (eds). 2021. *Criminal Law Reform Now*. Oxford: Hart Publishing. pp1-24.
81. Table Q 5.3 https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2021.
82. https://www.sfo.gov.uk/download/annual-report-and-accounts-2020-2021.

were no identifiable victims in the cases where Confiscation Orders were made. In 2021-22, £136,000 was paid in compensation to victims.

A broader dataset can be found in the CSEW 2021 which measures frauds against individuals only: we have included the losses to individuals from computer misuse, though they go beyond our formal brief, because they may be of interest; see Table 9. There are other mechanisms by which fraud victims can be recompensed for their losses. The Financial Services Compensation Scheme (FSCS) is not a compensation scheme for fraud victims alone: it is an industry collective levy on authorised persons used to compensate those who have lost money to FCA-authorised bodies, as happens for example when an insurance company goes bust for business reasons unconnected with fraud.

Table 9. Fraud and computer misuse by loss (of money or property) - number and rate of incidents and number and percentage of victims, aged 18 and over

Offence group	Number of incidents (thousands)	Rate per 1,000 adults	Number of victims (thousands)	Percentage victims once or more
FRAUD [note a].[83]	**5,035**	**109**	**3,947**	**8.6**
With loss, no or only partial reimbursement	1,324	29	1,042	2.3
With loss, fully reimbursed	2,211	48	1,849	4.0
Without loss	1,500	33	1,283	2.8
Bank and credit account fraud	**2,868**	**62**	**2,239**	**4.9**
With loss, no or only partial reimbursement	564	12	373	0.8
With loss, fully reimbursed	1,612	35	1,320	2.9
Without loss	691	15	597	1.3
Advance fee fraud [note b]	365	8	342	0.7
With loss, no or only partial reimbursement	62	1	59	0.1
With loss, fully reimbursed	17	0	16	0.0
Without loss	287	6	267	0.6
Consumer and retail fraud	**1,510**	**33**	**1,315**	**2.9**
With loss, no or only partial reimbursement	615	13	539	1.2
With loss, fully reimbursed	558	12	509	1.1
Without loss	337	7	304	0.7
Other fraud [note b]	**293**	**6**	**231**	**0.5**
With loss, no or only partial reimbursement	83	2	78	0.2
With loss, fully reimbursed	24	1	22	0.0
Without loss	185	4	137	0.3
COMPUTER MISUSE	**1,772**	**38**	**1,564**	**3.4**
Computer virus [note c]	**406**	**9**	**352**	**0.8**
With loss, no or only partial reimbursement	111	2	92	0.2
With loss, fully reimbursed	0	0	0	0.0
Without loss	295	6	264	0.6
Unauthorised access to personal information (including hacking)	**1,366**	**30**	**1,224**	**2.7**
Unweighted base - number of adults	39,042		39,042	

Source. Home Office CSEW 2021

Therefore, it is not an easy task to strip out fraud from loss. Indeed, the Financial Services Compensation Scheme (FSCS) 2021 Outlook Report does not mention the word 'fraud' but notes that of the £900m levy currently forecast, about £400m relates to compensation for failures that have not yet occurred.[84] Its Annual Report mentions risks of internal fraud (because it is an accounting document for the agency) but otherwise notes that it had made recoveries for claimants of £280 million since April 2016, and paid out £584 million in compensation 2020-21, including £4 million for people whose losses exceeded its compensation limits (which are currently £85,000 per person).

5.5 SUMMARY

Both individuals and businesses are victims of fraud and suffer harm across a range of issues from fear to financial loss, disruption of normal commercial activities and concern about online and other platforms. Given the numbers of cases referred to the police 'pursue' function, significant numbers lose what may appear relatively small amounts, but some may cause greater levels of harm to those involved and raise levels of fear or concern over ongoing risks from the processes that led to the original fraud. Predictive models of who is likely to be harmed the most are at an early stage.

Controversy continues over financial regulator liability for compensation in some cases – an impetus for active regulation - but for significant numbers of victims, the sums recovered are very modest absolutely and as a proportion of losses. Largely in higher value cases, where the victims have enough resource to sue themselves or through third party litigation

83. Notes are as follows: (a) The 'with loss' categories relating to fraud refer to financial loss, including money stolen and additional charges or costs incurred, as well as loss of property or goods; (b) In the large majority of cases of loss relating to 'advance fee fraud' and 'other fraud', victims received no or only partial reimbursement, as the nature of such frauds makes full reimbursement less likely; (c) Loss through computer viruses is mainly associated with additional charges or costs incurred as a result of the virus (e.g. repair/replacement costs), which are less likely to be fully reimbursed.
84. *Outlook November 2021*, London: FSCS.

funding, more will have been recovered by civil lawsuits from plaintiffs, though some of these are recoveries from financial intermediaries or regulators rather than from the alleged fraudsters. But though no recent surveys have been done assessing their impact on public or business, recoveries may provide some public reassurance as well as harm mitigation. This takes us to the next question about perceptions of fraud, the configurations of responses and the effect of those configurations on the public's perceptions of the police 'pursue' function.

6. PUBLIC PERCEPTIONS OF FRAUD AND POLICING

6.1 Fraud as a Serious Issue

Research in the UK, US and Australia consistently demonstrates that the public views a range of frauds – including frauds against business - seriously. Decades ago, reporting on their study of police and public perceptions of crime seriousness in Greater Manchester and in Devon & Cornwall, Levi and Jones[85] observed that although the general public viewed a set of fraud offences very seriously compared with burglary and car crime, there was no automatic link between these crime seriousness rankings and either policing or sentencing preferences (which were not investigated in that study). This remains the case: thinking something serious does not mean you want a lot more policing or tougher sentences (or that the latter will always reduce the harms, however satisfying they may be to our feelings of justice or reassurance).

It is possible that one reason why people who are bothered about fraud may not press for its being a police priority is that they have been led to expect that the police could not deal with frauds very effectively. The lack of fraud data appearing on the 'crime in your area' www.police.uk websites is unlikely to influence this perception that fraud is not the police's business: but we regard it as a highly regrettable, almost ludicrous side effect of national reporting via AF that even the City of London police area apparently experiences no fraud![86] A government analysis of existing data in 2017 reported that only 17% of CSEW fraud was reported to the police or AF, with reporting rates showing only slight variations by fraud type. The main reasons for this were: 'never heard of AF' (66%); 'thought it reported by another authority' (15%); 'other' (8%); 'too trivial/not worth reporting' (5%); 'dealt with matter myself/ourselves' (4%).[87]

Nevertheless, as with voting, pressures from the public influence the politics of policing. There is surprisingly little information on the public's views about policing priorities, and anyway, policing leadership sometimes requires decisions that are contrary to current public views, especially since -television documentaries notwithstanding - large sections of the public are not well informed about the complexities of police work or criminal justice or how they actually respond to crimes.

Looking more generally at perceptions of being protected by the state, an Ipsos MORI survey in September 2021 showed only 7 % of the public were very confident and 32% confident that government and law enforcement would protect them from fraud and cybercrime: very slightly less confidence than about protection from crime generally.[88] This was consistent with their expectations that they were likely to be victims of a range of frauds and cybercrimes in the next year.

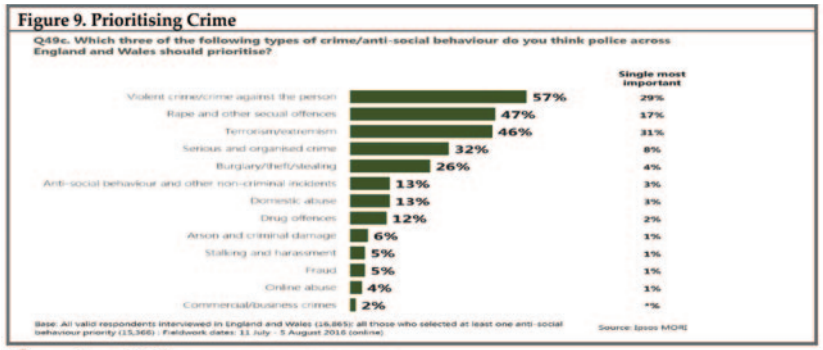
6.2 Perceptions of and Potential Impact of the 'Pursue' Function

The most relevant data are found in work done by Higgins for the Police Foundation in mid-2019 as part of a focus group study of some 250 people from seven PCC areas, which did not include any large Metropolitan areas.[89] The methodology of this prioritisation is set out below.[90] In an earlier national representative survey of 17,000 people in mid-2018, only 5 percent of the public – see Figure 9 - wanted the police to prioritise fraud, and two percent wanted them to prioritise crimes against business (compared with 32 percent who wanted 'Serious and

85. Levi, M. and Jones, S. 1985. 'Public and police perceptions of crime seriousness in England and Wales'. *British Journal of Criminology*, 25. pp234-250. For a deeper general analysis of problems in crime harm assessment, see Greenfield, V, and Paoli, L. 2022. *Assessing the Harms of Crime*. Oxford: Clarendon Press.
86. https://www.police.uk/pu/your-area/city-of-london-police/community-policing/?tab=Statistics.
87. Blakeborough, L. and Correia, S. G. 2018. The scale and nature of fraud: a review of the evidence. London: Home Office. The public awareness may have changed since then, even if much media coverage of Action Fraud has been uncomplimentary.
88. https://www.ipsos.com/en-uk/almost-half-uk-adults-expect-crime-uk-go-over-next-year.
89. Derbyshire, Dorset, Gwent, Hertfordshire, Humberside, Northamptonshire and Nottinghamshire.
90. See Higgins, A. 2020. *Policing and The Public: Understanding Public Priorities, Attitudes and Expectations*, Insight Paper 1. London: Police Foundation. Figures 6 and 8. At the start of each focus group (before any substantial discussion of crime and policing issues had taken place), each participant was provided with 48 'items' printed on magnetic cards (shown on the left), and asked to arrange them into a 'Q-sort' grid in the order that best represented their views on what 'the police should prioritise'. The grid required two items to be designated as 'top priorities' (each given a ranking score of 9), four to be assigned to the next highest priority category (score of 8), six in the next category (score 7), eight in each of the next three descending categories (scores of 6, 5 and 4), six in the score 3 category, four in score 2 and two in the (lowest priority) score 1 category. As an illustrative summary of the views most frequently expressed by study participants, Figure 6 shows the mean ranking score given to each item (on the right) and the proportion of respondents giving each a 'high' (7-9), 'medium' (4-6) and 'low' (3-1) priority ranking (in the bar chart). The data were also subjected to force-level and second-order factor analyses to identify the distinctive shared 'viewpoints' present within the sample (see further Higgins, A. 2019 *Understanding the public's priorities for policing*. London: The Police Foundation).

Organised Crime' prioritised, which in the minds of some respondents might have included fraud:[91] this possibility was not explored, though fraud is part of the UK government SOC Strategy and is among the 2022 priorities of the Director General of the National Crime Agency[92]).

Figure 9. Prioritising Crime



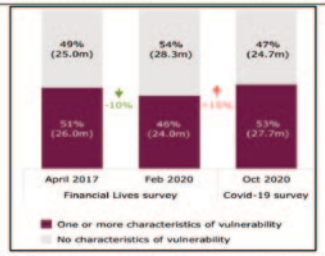
Source: Ipsos MORI

Looking only at the 'Pursue' issues, the focus groups in mid-2019 concluded that 'Targeting those who commit online frauds and scams' was well down the priority scale, though fraud might have been featured implicitly within the higher placed other policing roles of looking after victims and building a stronger resilient community. 14.2 per cent of people put targeting online scammers as one of their top three policing priorities; and after discussing a range of crime issues within focus groups, 2.6 percent gave targeting online scammers a higher and 6.4 percent a lower priority than when they began their deliberations. (Tackling organised crime, of which some fraud is or ought to be a part, was viewed more seriously after group deliberations.)

Earlier research looking specifically at the expectations of fraud victims has found that victims place a high value on getting their money back and seeing an offender brought to justice.[93] As the Police Foundation noted in reviewing research into victims, 'we shall see below these fairly minimal expectations of fraud victims (being kept informed, a sympathetic hearing, a single point of contact and support to get over the experience) are very far from being met in practice'.[94] This issue is also linked significantly to repeat victimisation and vulnerability, and the dynamics of fraud also suggest that the recent Covid-driven environment and the pervasive dependence on the internet for a range of retail and other services have also changed the dynamics of susceptibility and future risk that are likely to be exacerbated by perceptions that there will be no compensation for loss or reassurance about future protection.

The Financial Conduct Authority has warned that that all customers are at risk of becoming vulnerable, but this risk is increased by having 'characteristics of vulnerability'.[95] These could be poor health, such as cognitive impairment, life events such as new caring responsibilities, low resilience to cope with financial or emotional shocks and low capability, such as poor literacy or numeracy skills. Its 2020 Financial Lives Coronavirus Panel Survey demonstrates that more consumers found themselves in vulnerable circumstances due to the pandemic, with 53% of adults displaying a characteristic of vulnerability (see Figure 10).

Figure 10. The Financial Conduct Authority Survey on Vulnerability between April 2017 and February 2020



Source. FCA. 2021. *Financial Lives Survey 2020: The Impact of Coronavirus.* London: Financial Conduct Authority. P64

It argues that not all customers who have these characteristics will experience harm. But they may be more likely to have additional or different needs which could limit their ability to make decisions or represent their own interests, putting them at greater risk of harm. So, the level of care that is appropriate for these consumers may be different

91. Ipsos MORI. 2017. *Public Views of Policing in England and Wales 2016/17*. London: Ipsos MORI. p19.
92. Personal communication.
93. Button, M., Lewis, C., and Tapley, J. (2009). *A better deal for fraud victims: Research into victims' needs and experiences*. London: National Fraud Authority. See also Skidmore, M., Goldstraw-White, J. and Gill, M. 2020. 'Vulnerability as a driver of the police response to fraud'. *Journal of Criminological Research, Policy and Practice*, 6:1. pp 49-64.
94. Police Foundation. 2018. *More Than Just a Number: Improving the Police Response to Victims of Fraud*. London: Police Foundation. p42.
95. https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers.

from that for others. These points are valuable, evidence-based insights, to be acted upon by the FCA and others: but they increase the range of 'vulnerable people' to a proportion of the general population that it is unrealistic for law enforcement or third sector bodies to intervene with as primary, secondary or tertiary prevention.

While neither published research nor police records nor crime surveys tell us much about the general distribution of fraud repeat victimisation, we do know from burglary and violence that this has important policy and practice implications, e.g., for safeguarding and 'vulnerability'. The dimensions of harm are also complex, and the relationship is not well understood, with plausibly important factors such as subjective feelings of abuse of trust, gender, age and the 'affordability' of the frauds in the financial situation of the victim.

6.3 SUMMARY

This section has noted the expectations and perceptions of the police role (and wider findings supported a preference for more community-oriented policing, though people may mean different things by that). It has also noted the limitations on what police can respond to, it being likely that significant numbers of victims will be left without resource to support them emotionally or financially, guidance and some indication of the outcomes of their reporting. Realism suggests that notwithstanding the fairly high probability that people will become victims of fraud – around 1 in 12 people annually - 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 in the minds of the public as well as in the minds (and effective caseload) of the police.

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. Reflecting the drivers for taking a public health approach, we have obtained as much secondary quantitative data as possible, allowing us to explore current and past interventions against frauds of different types. It must be admitted that hitherto, the evidence of impact resulting from experiments is weak.

7. THE IMPLICATIONS FOR POSSIBLE INTERVENTIONS

7.1 Considering a Public Health Approach to Fraud

This study starts with the premise that though all cases have deception in common, fraud is not a homogeneous form of behaviour, nor are all frauds equally harmful. The financial size of a fraud loss is not the same as the impact of the loss, and nor does it fully predict the loss of trust in the medium (e.g., online banking) through which the fraud occurred. Not all fraud is driven by 'organised crime groups' (OCGs) as conventionally understood,[96] and though fraud collectively may be a national (and human) security issue, this is not particularly helpful in dealing with individual or aggregated frauds at a local or regional level. Most terror incidents are designed to cause huge attention and harm; most frauds (and other crimes for gain) are not, and fraud has not hitherto produced enough 'noise' to counter the threat collectively. The general evidence to date shows that fraud victims span the full spectrum of ages and income/wealth, ethnicities and genders, modes of being defrauded, levels of loss and likelihood of recovery. Further, whereas the majority are victims only once, a significant proportion – over a third for most categories - are multiply victimised by frauds of the same or of different types.

Our earlier 2015 analysis of national Action Fraud (AF) data[97] showed the complex and highly differentiated landscape of fraud: the median amount lost to fraudsters across all fraud types at that time – 2013-2014 - ranged (at historic prices) from £112 via misuse of contracts in the telecom industry, to £38,974 from pension fraud.[98] Those categories with the biggest losses – such as pensions, business trading and financial investment frauds – were those where cyber-enablement or cyber-dependency was a relatively modest factor. Conversely, while offences with significant cyber-involvement seemed to vary in both number of cases and average loss, the data also showed that little money lost from frauds was likely to be recovered for the victims, especially not from the offenders (as opposed to from the banks and other intermediaries).

Even if a 'reasonable' amount of extra resources were available to the police for fraud investigations, this alone would probably not reduce substantially the levels of such crime, unless the criminality was highly concentrated and difficult to copy. Indeed, we would argue that a public health approach should be considered because of the pervasive nature of 'fraud', within which there are many variations in terms of likelihood, loss, harm[99] and involvement of specific groups (and the availability of data to allow us to identify these). The need is strengthened by the low possibility of resolution through criminal justice approaches, the need to involve different agencies and different intervention points, involving awareness and self-driven prevention – hence failed attempted frauds - and involving engagement with formal partners, businesses and others to reduce the occurrence (and re-occurrence) of fraud.

As also with general and terrorist violence reduction, the public may not even be aware of interventions that reduce their risks, before and after individuals or organisations become victims. 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 and to reduce crime levels. Traditional investigations and prosecutions do have an important role to play, not just for public reassurance reasons but to ensure greater justice and to reduce some offenders' willingness and ability to act harmfully: but we need to be clear about its limits and have a frank public discussion about what to prioritise for this, given scarce resources. A single economic crime or fraud agency will not solve this problem, either nationally or for any given police area.[100]

96. Or as measured in the Home Office Management of Risk in Law Enforcement (MoRiLE) based scoring model to determine prioritisation in organised crime cases.
97. See Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. 2015. The Implications of Economic Cybercrime for Policing: Research report, City of London Corporation. City of London Corporation. https://orca.cardiff.ac.uk/id/eprint/88156/1/Economic-Cybercrime-FullReport.pdf.
98. We used median values because the averages are skewed by large standard deviations, and often estimations of loss. The advance-fee payments, for example, many of which are cyber-enabled, are numerous and yield relatively small amounts to fraudsters. The data field is skewed because of a few very large frauds, so, to correct for these, the median has been used to demonstrate the difference. This is discussed and illustrated in the WMP Area Fraud Report.
99. Harm is affected not only by our intentional efforts, and some intervention efforts are unsuccessful, though we may not always understand their (in)effectiveness, or even sometimes be uninterested in learning how ineffective they are, for example when there is an organisational imperative to 'do something'.
100. See House of Commons Treasury Committee. 2022. *Economic Crime*. HC145. London: House of Commons.

Retrospective interventions after the event are only a small part of a population-based response. This has been long recognised in interventions within the framework of the Four Ps – Prevent, Protect, Pursue and Prepare – now used generally within law enforcement. However, there is relatively little systematic information about the rationale, choice, extent, forms and balance between the 4 Ps in determining counter-fraud interventions or their effects, particularly not on their effects on levels and/or the organisation of crime.[101] The analogy with health outcomes might be fruitful, especially in this pandemic/lockdown era where it is appreciated that mental well-being is an important but partly independent component from physical/financial harm.

Thus, refined by an understanding of who is more and who is less 'at risk',[102] we might shift the approach to fraud on to a community-wide preventive approach with the aim to 'satisfice' (sufficiently satisfy) the public and victims with a not wholly scientific mix of general preventative measures (Protect), post-victim resilience (Prepare), and classic investigations (Pursue), alongside public reassurance that their concerns are being paid attention to (an important component of harm reduction omitted from the Four Ps), and efforts to reduce the numbers and intensity of willingness to defraud (Prevent). The optimal mix depends on what the objectives are, and these remain relatively ill-defined, despite important developments such as HMG's Economic Crime Plan, which requires revision to something more strategic and less programmatic when redeveloped and published in 2023. Also, they depend on capacities and capabilities, and the willingness to collaborate, which vary between sectors over time and place, as is almost always the case in every sphere of life. Finally, the optimal mix depends on the availability of evidence from trials of interventions, preferably experiments supplemented by observations so that theories of change can be better understood.

7.2 Devising Interventions in a Fraud Context

We recognise here that frauds are not the same as health issues and that the simple transfer of a public health approach is not possible. On the other hand, the conceptual thinking behind a public health approach and its core components does provide us with a framework within which to consider a significant shift in dealing with frauds through a communitywide approach, through a focus on prevention and on wider networks of implementing agencies – all with the intention of, to paraphrase the NHS Long Term Plan, reducing the demand for and delays in treatment and care within the criminal justice system. So, let us first remind ourselves of the public health intervention types – individual, relationships, community and social – within primary prevention (taking action to reduce the incidence of disease and health problems within the population, universal or targeted); secondary prevention (systematically detecting the early stages of disease and intervening before full symptoms develop); and tertiary prevention (softening the impact of an ongoing illness or injury that has lasting effects).

Fraud prevention has not just arrived now. Corporate Audits (internal and external) have long been a form of both primary and secondary prevention and – where they fail to stop fraud – may offer the external auditors as 'deep pockets' to be sued even if compensation cannot be got from the alleged fraudster. At the individual level, many of us have been phoned by our payment card issuer to ask proactively if transactions are ours, because the issuer has detected an anomaly in our pattern of purchasing. This was particularly important before Chip and PIN made it harder for fraudsters to clone cards and use them internationally.[103] Our smartphones offer some level of device control and the rise of two-factor authentication where we are asked to approve payments in-app acts as a brake on fraud. On the other hand, there are other areas of fraud where controls are much weaker, while widespread internet and smartphone use – accelerating during the pandemic - have made vulnerable a much larger proportion of the population.

Moving away from high volume frauds, we must also remember the importance of organisational culture (private and public sector) in which domineering senior executives or ill-supervised lower/mid-level staff can

101. It is quite possible to reduce the concentration of criminality within offender networks without reducing the total volume of crime.
102. We express it this way because it is difficult to see from the CSEW and FCA data any substantial sector of the individual or business population who are not in any meaningful sense at risk of being victims of some type of fraud or scam over their lifetimes. This issue needs to be explored further.
103. Levi, M. and Handley, J. 1998. *The Prevention of Plastic and Cheque Fraud Revisited*. Research Study 182. London: Home Office.

override procurement or dealing room systems, and personal assistants can be conned electronically into 'urgently' purchasing high values of Google/Apple Play gift cards at the urgent requests from people they mistakenly think are their bosses. And changing situational triggers – e.g., Covid-19, rising energy and other costs of living, high inflation eroding the real inflation-adjusted value of savings, apparent 'guarantees' from 'authorised firms' – offer fraudsters a variety of traps for us.

As we have demonstrated, fraud interventions lie within a complex ecosystem. In the private sector, some are mandated by sectoral agreements usually concluded under pressure from media, politicians and/or regulators; some are largely voluntary, chosen to reduce avoidable losses which, if commonly experienced, can lead to data sharing and joint action, e.g., not-for-profit Cifas and card issuer and acquirer data sharing; cross-sectoral bodies like Stop Scams UK. There has been some spill-over benefit from measures taken to deal with money-laundering – for example in combating money muling which distributes proceeds of fraud – if not as much as might be expected if Anti-Money Laundering controls functioned better: it should be harder to set up new or operate existing money mule accounts if Customer Due Diligence were applied rigorously. In the public sector, changes have been less common, as counter-fraud measures have often been built only weakly into large system changes such as online tax submissions, VAT registration and repayments, Universal Credit, the right to cash in private pensions, and Covid-19 business loans and grants, as well as into emergency public procurement of Personal Protective Equipment. The FCA has been heavily criticised for its slow interventions against a succession of major frauds or alleged frauds and areas such as peer-to-peer lending, and only recently has shifted its strategy in a 'public protection' direction, which includes improving financial literacy and warnings about cryptocurrency investments and investment advice given via social media.[104]

Notwithstanding the welcome growth of the public sector as well as the private sector counter-fraud profession, counter measures usually come only after very significant losses have occurred. And as the UK taxpayer is already experiencing in 2022 in the search for unpaid Bounce Back Loans, criminal or even civil tax asset recovery consumes far more resources and is much more uncertain than prevention. (Though effectiveness measurement of prevention is often challenging, especially before large visible losses have occurred: demonstrating the counterfactual is very difficult.) Such before-and-after fraud loss and fraud volume measurement and observations/theories of change are central to reviewing interventions in the Public Health approach: but investment in them in the economic crime sector has been very modest compared with medicine. Very few randomised control trials or quasi experiments have been attempted to date, though it might be feasible for banks and police to randomly allocate interventions (including victim care) and evaluate the impacts on levels of fraud, repeat victimisation and victim welfare, once ethical approval is given; and careful observational case studies and natural experiments can give valuable insights.[105]

Formal police-private sector anti-fraud collaborative meetings have been going on for over 20 years[106] (and informal ones for longer), and the City of London police have been strengthened by investment from the banking and insurance industries and the Intellectual Property Office to ensure a more consistent and efficient police response from separately funded dedicated squads in a limited number of serious cases. However outside of these, change within the police has often been glacial, inhibited by a lack of longevity in roles, weak responses to changes in fraud victimisation, abstractions to other urgent duties, and lack of critical mass to make a sustained and visible impact. We have yet to see some of the impacts of recent short-term funded efforts to enhance collaboration between Trading Standards and the police: but these need to be informed by appreciation of the different vectors of staffing and incentives in the resource-starved local authorities, and asymmetry between police and local authority geographical boundaries. Such collaborative efforts in public-public as well as public-private partnerships might be expected to affect all levels of public health.
Some areas of fraud are less amenable to public-private collaboration.

104. 'Young investors look to social media, so FCA follows suit', *The Times*, 18 June 2022.
105. Prenzler, T. 2019. 'What works in fraud prevention: a review of real-world intervention projects'. *Journal of Criminological Research, Policy and Practice*. 6:1. pp83-96.
106. Levi, M. 2010 'Public and Private Policing of Financial Crimes: the Struggle for Co-ordination'. *Journal of Criminal Justice and Security*. 4. pp343-357. https://www.fvv.um.si/rv/arhiv/2010-4/Levi.pdf

The HBOS Reading systemic exploitation of small businesses deemed to be in need of banking support consumed huge Thames Valley police resources and continues to generate tensions not just over who does and should pay for major police investigations, but also in compensation payments two decades after the frauds began.[107]

Keeping in mind the heterogeneous contexts of different sorts of fraud, fraud levels experienced today are a product of three elements: (1) the expertise & resources of offenders; (2) the efforts, skills and resources of third parties and potential victims to monitor and intervene when fraud is suspected; and (3) the opportunities offered to would-be offenders by victims and potential victims by the way the public and organisations go about their daily and financial lives. Some fraud threats are purely from external people; some are from people internal to organisations; and others are mixed. For example, UK Finance states:[108]

> 'Investing in advanced security systems to protect customers from fraud, including real-time transaction analysis. The industry prevented £1.4 billion of unauthorised fraud in 2021, equivalent to 65.3p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.'

Cifas states that its interventions have reduced fraud by £1.4 bn. This is not the place for an extended analysis of fraud controls: we will instead restrict ourselves to the kinds of measures that a PCC might propose for the police, enforcement partners, businesses and individuals. It is useful to divide frauds up into three broad categories: frauds against the individual; frauds against business; and frauds against the public sector. The latter are largely left to specialist agencies, except where specific police powers are needed.[109] For frauds against the individual, we might divide these between those whose victims are (at least in principle) entitled to compensation from a general compensation fund (e.g. the FSCS or The Pensions Regulator) or from their bankers, and those not entitled to such compensation: the lack of compensation entitlement is often because their investment was not with an authorised person or firm, though they may have thought or simply assumed that the person/firm was authorised (i.e. they lie 'outside the perimeter', in traditional regulatory language). The FCA are now expected to be active in closing down people who falsely claim to be regulated by them, or who exploit loopholes in the regulatory process; and larger social media firms have recently agreed to check such claims of authorisation before advertising them. These dimensions and sub-dimensions of fraud victimisation would need to feed into a framework for giving shape to a public health approach.

These are the sites of ongoing financial battles between victims, media, activists, and those (mainly banks and their customers & investors) who are called upon to compensate. Some of these battles are cultural, summoning up conscious or unconscious beliefs about 'just deserts', 'prudence' and 'recklessness' on the part of victims. One important element also that arguably should inform prioritisation decisions is the affordability of frauds to individuals and to businesses: a term that may be wrapped up in 'vulnerability', which requires greater clarity of use since different organisations may have different constructs of what it means, though the word is the same. It remains common to think in terms of money losses, which unintentionally prioritise the wealthier (or perhaps formerly wealthier) people who lose the most in money terms. But a more meaningful if operationally difficult perspective is to analyse losses in terms of the wealth and present/future income of losers, which measures their financial resilience better: the evidence is not clear on whether financial and emotional resilience are correlated. In a practical context, it might be greeted with resentment if the police asked for information equivalent to that required by an authorised financial adviser before deciding whether or not to take on a case, so some simpler indicators may be required. Harm is not the only criterion, at least for the Pursue function: investigatability and prosecutability using information and defendants from abroad are also central if there is going to be a Pursue intervention, though apart from careful analysis of crime scripts and modus operandi of the frauds (and incapacitation of offenders), offender detection and bringing to justice is not important for Protect or Prepare.

107. It is claimed that this fraud involved nearly £1 billion and cost the Thames Valley police £7 million (£5 million net of Home Office subsidy) to investigate: https://www.thamesvalley-pcc.gov.uk/news-and-events/thamesvalley-pcc-news/2018/01/statement-from-the-police-and-crime-commissioner-fraud/ (Accessed 2 February 2022). Lloyds Bank's compensation for victims may finally have been resolved in June 2022.
108. https://www.ukfinance.org.uk/news-and-insight/press-release/cross-sector-action-needed-criminal-gangs-steal-billions. This is plausible, though the internal data are unavailable for inspection.
109. The cost benefit of average and marginal investigative resources varies significantly between public sector bodies such as DWP and HMRC or between the SFO and CPS: but this lies outside our brief here.

7.3 Current Intervention Types

There are a growing number of interventions aimed at impacting potential fraud victims, ranging from charities to regulators.[110] Project Bloom - renamed in late 2022 as the Pension Scams Action Group - was created in 2012 and brings together government departments, agencies, regulators, law enforcement bodies and representatives of the pension industry to tackle pension scams, rising as a by-product of government rule-changes and falling interest rates. As well as the FCA, MaPs and TPR, partners include the Department for Work and Pensions, HM Treasury, the Serious Fraud Office, City of London Police, the NFIB, AF, the Pensions Scams Industry Group, the Information Commissioner's Office, the Insolvency Service, National Trading Standards and the National Crime Agency. (Regulation exists to reduce damage from non-fraudulent losses and corporate failures as well as from fraud.) However, research noted that there was scope for much better information sharing and coordination of action, and that 62 percent of consumers proceeded to transfer their pension to scammers even when warned of the risks.[111] We are pleased to see the regulations in force since end November 2021 by DWP of amber and red warning flags to try to inhibit Pension Liberation Frauds before pension transfers are allowed.[112] The credibility of official agencies and third parties as well as the cognitive processes of potential victims are critical issues for future research and for the impact of counter-fraud measures. Poor information is publicly available about failed attempts at fraud, from which we might learn.

Enormous progress has been made in opening up interventions in the retail banking and e-commerce space, and in efforts to close down online scams, especially from phishing attempts (see National Cyber Security Centre reports), but criminological evidence suggests that many dark market and other websites soon re-emerge after disruption. So 'effectiveness' can depend on our time horizons, and activities that may provide public and media reassurance may have far less impact on future offending levels, while other efforts may be abandoned if they do not show quick results: patience in crime reduction efforts has often been difficult to achieve. Indeed, a Scottish review of UK evidence noted that 'there is no robust evaluation evidence as to the success of these initiatives as many of the interventions are quite recent and still current, with no processes in place to measure impact. In fact, we are not aware if any of these initiatives have any indicators which are being measured.'[113] This also applies to many promising interventions that have understandably won praise in the annual UK Tackling Economic Crime Awards.[114] To the extent that Public Health approaches rely on Randomised Controlled Trials and quasi-experiments, very few initiatives indeed would count (though advocates of 'realistic evaluation' would add other methods, which we support). To the extent that commitment, cooperation and charisma are part of success – and their absence is part of failure – we are sceptical that many positively evaluated tests may work as well when rolled out as they do in the experiments: this is a human feature of success and failure that is important to account for in the evaluation process.

Prevention efforts also can come from individual efforts, perhaps stimulated by advertising and feedback from banking 'apps' which make it easier to get automatic information about expenditures and that enable temporary account freezes. The Financial Lives Survey found that most adults are careful with their cards and account details (or – more accurately – they say they are careful).[115] Two-thirds (65%) say they always check their statements for unfamiliar transactions. Similar proportions always dispose of their statements and documents securely (63%) and always cover their PIN when withdrawing money or using their cards to pay for goods (62%). Three-fifths (60%) always check if an internet site is secure when giving their bank or credit card details. However, those least likely to take these precautions include younger adults aged 18-24 and older adults aged 75+. Beyond card fraud risks, Financial Lives noted that almost one in five of all UK adults experienced one or more unsolicited approaches about investments, pensions and

110. ScamSmart resources | FCA.
111. Skidmore, M., 2020. Protecting People's Pensions: Understanding and Preventing Scams. London: Police Foundation.
112. https://www.gov.uk/government/consultations/pension-scams-empowering-trustees-and-protecting-members/pension-scams-empowering-trustees-and-protecting-members-consultation; Which? Money, January 2022.
113. Scottish Government/ EKOS Limited. 2021. *Preventative Spend Research 2018. Edinburgh*: Scottish Government. p9.
114. https://thetecas.com/. Full disclosure: the first author of this report was the first recipient of a Lifetime Tackling Economic Crime Award. But we are thinking here of the individual and team categories.
115. Financial Conduct Authority.2021. *Financial Lives Survey*. London: Financial Conduct Authority. Ch8. There is always a validity problem with self-reported data on public health and on crime prevention. People do not always do what they say or believe they do!

retirement planning which could potentially be a scam in the 12 months to February 2020. A million of these adults responded to an approach and a tenth of those paid out money: that is a high rate of annual attempted and successful crime risk, and suggests to us the importance of outreach to potential victims, an issue taken up by the FCA's recent strategy review, but not with details of how it will be done beyond warning adverts.

Fraudsters have taken advantage of Covid 19. Almost half of adults said they have had more unsolicited approaches about investments, pensions and retirement planning which could potentially be a scam between March and October 2020. Over one-third (36%) received one or more Covid-19 related unsolicited approaches which could potentially be scams. Examples include approaches designed to look like they are Government offers of Covid-19 or Energy costs financial support, from the NHS Test and Trace service, from TV Licensing or from HMRC (though these subsequently declined after campaigns and website take-downs). 1.4 million people say they paid out money after an unsolicited approach involving Covid-19. Although there have been many advertisements of warnings, we know little about their cognitive longevity and when they may need a booster. Unfortunately, there is no vaccine available against fraud, as is demonstrated by the Theranos case in which many clever elite individuals and businesses lost a great deal of money (which they could easily afford), investing $945 million in innovative blood-testing which never worked and never plausibly could work.[116] Likewise, sophisticated as well as unsophisticated investors have lost money in some crypto-investment firms such as FTX, which failed at the end of 2022, when its business once valued at $32 billion became almost worthless. One hypothesis is that clever people are as swayed as others by personal attractiveness and by transformational narratives, especially when combined with endorsement by people they respect as shrewd and/or community leaders. This is a characteristic of many Ponzi schemes and affinity frauds, most emblematically in the Bernie Madoff case.[117]

7.4 Recovering the Proceeds of Fraud

Overall, 1.9 million British adults lost money to fraud in the 12 months to February 2020, as the Financial Lives survey showed. Of these, 65% fully recovered it, 13% recovered some of it, 8% tried but failed to recover it, 5% did not try to recover it and 5% had not tried yet. Serious Fraud Office and Crown Prosecution Service data are not broken down by geographic area, but their fraud cases mostly come from the police and the financial regulators. Despite the banking protocols, compensation for victims of authorised push payment fraud remains a contested space, with allegations about some banks being insufficiently tolerant of customer foolishness appearing at least weekly in the press. However, though it is a well-publicised issue, this represents only a modest percentage of total fraud losses.

Of the £354 million recovered in total from Confiscation Order, Forfeiture Order and Civil Recovery Order receipts in 2021 to 2022:[118]

- **£154 million was recovered through Confiscation Order Receipts**, a 56% increase from 2020 to 2021, but only 4% higher than the 6-year median amount recovered based on nominal values i.e., not adjusted for inflation
- **£191 million was recovered through Forfeiture Order Receipts**, a 76% increase from 2020 to 2021 and the highest amount recovered in the last six years, explained by high value Account Freezing Orders and Cash Seizures, which reached record highs of £115m and £74.3m respectively, based on nominal values i.e., not adjusted for inflation
- **£9.8 million was recovered through Civil Recovery Order Receipts**, a 23% decrease from 2020 to 2021, but 11% higher than the 6-year median amount recovered, based on nominal values i.e., not adjusted for inflation
- **£23 million was paid in compensation to victims** from proceeds of crime recovered through Confiscation Order receipts in 2021 to 2022, a 37% increase from 2020 to 2021, but a 27% decrease from the 6-year median, based on nominal values i.e., not adjusted for inflation, which is linked to the overall decline in Confiscation Order Impositions and subsequent receipts which have fallen in the same period. In 2021-22, £136,000 compensation was paid to victims from Serious Fraud Office cases.

116. Carreyrou, J. 2019. *Bad Blood: Secrets and Lies in a Silicon Valley Startup*. London: Picador.
117. Henriques, D. 2017. *The Wizard of Lies: Bernie Madoff and the Death of Trus*t. London: St. Martin's Griffin; Springer, M. 2020. *The Politics of Ponzi Schemes: History, Theory and Policy*. London: Routledge.
118. Asset recovery statistical bulletin: financial years ending 2017 to 2022.

To incentivise asset recovery from all crimes, £142 million of ARIS funding was distributed to Proceeds of Crime Act 2002 Agencies in 2021 to 2022, a 60% increase from 2020 to 2021, which is mirrored by the overall increase in the proceeds of crime recovered in the same period. In 2020/21, the SFO's proceeds of crime team confiscated £5.7m worth of illicit assets, rising to £45m in 2021/22. The SFO also secured £1.2m from a luxury West London apartment which it showed to have been partly purchased with the corrupt funds of its owner's criminal conduct in Brazil. However, very little of this directly or perhaps even indirectly affects individuals or businesses in the West Midlands. As a proportion of fraud losses, these recovery sums are very modest (as is the case for recoveries from every type of crime for gain), and prosecutors' reluctance to invest in financially costly and risky Restraint Orders early enough is long standing pre and post-POCA 2002: the West Midlands PCC may as well await the government proposals that will follow from the Law Commission 2019 review. Some businesses may engage in civil litigation to recover funds from fraud – and this should be considered more widely, especially via litigation funding - but the elapsed time from frauds to reporting to action including late or no applications for Restraint Orders make improving non-cash recoveries challenging. Account Freezing Orders under the Criminal Finances Act 2017 have been increasingly employed by the police nationally, and those, plus measures to encourage banks to be more proactive in freezing suspect funds (especially from 'vulnerable people') remain the best hope of impacting recoveries in the short run. This is a recommended focus for the PCC in generating greater public reassurance and victim satisfaction. There are also issues of general access to and use of Suspicious Activity Report data in police investigations if better use is to be made of expensively acquired valuable financial crime data.

7.5 Moving Offenders away from Crime

The intention of targeted warnings is to deter recipients from beginning or continuing offending, by communicating to the recipient that there is a cost to their activities, and a consequence if they continue down a criminal pathway. Two key theoretical perspectives underpin intervention: deterrence and labelling:[119]

- Avoiding stigma and economic consequences of criminal record (and saving prosecution and court time!). Reintegrative shaming theory guides which sanctions are likely to be more, or less, stigmatising: those that focus on the wrongfulness of (and harm caused by) the act, rather than the characteristics of the offender, are considered to be more likely to reduce crime. Also helpful is procedural justice, whereby people's compliance with the law is conditioned by their perceptions of fairness and legitimacy, though this may have less effect on the offending of people who are already committed offenders;

- targeted warnings can prevent crime if the recipient perceives: (a) the warning is fair; (b) the cop or civilian who delivers the intervention is acting rightfully; and (c) the intervention is focused on the act rather than the actor;

- A recent Dutch study aimed to reduce distributed denial-of-service attacks by alerting/enhancing the consciences of relatively inexperienced Internet users, using a quasi-experimental design for four warning banners displayed as online advertisements and the contents of their two linked landing pages. The results suggested that social messages – i.e., emphasising the social consequences of DDoS attacks - may work better than traditional deterrent or information alone messages when engaging with potential cyber offenders.[120] Note that this experiment was not aimed at 'organised' cyber or economic offenders and should not be assumed to apply to them;

- Although cease-and-desist visits and targeted prevention messaging have been used in the context of cybercrime (e.g., by the NCA) and by trading standards, there is little known about how effective they are,

119. For a very useful overview of cybercrime issues, see Brewer, R., Maimon, D., de Vel-Palumbo, M., Hutchings, A., Holt, T., and Goldsmith, A. 2019. *Cybercrime Prevention: Theory and Applications*. London: Palgrave.
120. 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). See also Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., and Chua, Y. T. 2022). 'Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services'. *Policing and Society*. 32:1. pp103-124.

especially with more established offenders. A randomized controlled trial in Sacramento[121] found that intelligence led targeting of prolific offenders for formal warnings with follow up warnings from bespoke police teams led to reduced offending by them and by their co-offenders. However, this is a much more challenging 'ask' when the offenders are not embedded in the regional community, especially when they are overseas and expect that monitoring and intervention will be low.

In terms of past UK experience:

- In 2014, there was a UK-wide police investigation into Blackshades, a remote access tool designed to take over, control, and steal information from personal computers. The investigation resulted in 17 people being arrested and 80 receiving a visit from a police officer. Approximately 500 others received a warning letter advising that it was believed they had purchased the software and that using it could be illegal;

- In 2015, the database for the LizardStresser booter service, which provided DoS attacks for a fee, was compromised and leaked, containing customer details for those who had purchased attacks. Six purchasers were arrested. 50 others who had registered with the site, but were not believed to have carried out an attack, received a home visit from the NCA, and were told that denial of service attacks are 'illegal, can prevent individuals from accessing vital online services, and can cause significant financial and reputational damage to businesses'. They were also informed that 'committing cybercrime can result in severe restrictions on their freedom, access to the Internet, digital devices and future career prospects.'[122]

Many types of cybercrime are committed for money or peer recognition, so well-targeted cautions that increase offenders' perceived risk of detection could work. The likelihood of detection, not the severity of punishment, matters to many cybercriminals, so warnings highlight that low-level offenders are not necessarily anonymous online, increasing the perceived likelihood of detection. Other offline research shows positive effects of warning letters on general populations, both randomly allocated and without e.g., Behavioural Insights Team tax warning letters to low level tax avoiders. There is no public evidence of follow up or impact, but this is promising. However, care needs to be given, since personally administered warnings about behaviour that is seen to be legitimate may generate defiance and more delinquency in future.

Diversion evidence is weak for cyberfrauds. There is no empirical evidence conclusively proving the effectiveness of such positive diversions in cybersecurity (except for some 'master cybercriminals' later employed in consulting). These may be worth trialling and evaluating. However, it might be difficult to obtain support from industry or police for such schemes, given the security risks presented – it is a challenge to keep offenders (and victims) away from negative online influences. Challenging the justifications used by cyber-fraudsters through moral reasoning and cognitive restructuring might help: But it seems unlikely that this would be realistic and very effective in China, Nigeria, Romania or Russia, where empathy with victims in the Global North may be lacking. Desistance evidence depends on good data about fraud and cyber careers, and this is currently very modest everywhere outside the Netherlands. Most importantly, such studies have been conducted on very specific areas of cyber-dependent crimes, and they are not readily generalisable to forms of economic crime that are committed by more experienced and 'criminally committed' offenders. As with other spheres of public health evaluations, the data currently are too thin to permit us to be confident about 'what works' in some areas of fraud prevention.

7.6 Interventions: Issues in Adapting or Developing a Public Health Approach

As noted earlier, a public health approach may suggest a need for more officers and civilians from a wider range of law enforcement and other organisations to be deployed to deal with frauds of different kinds in different ways, along with appropriate resources and – as in requirements for local authorities to collaborate in public health – even mandatory requirements to implement counter-fraud plans. The low ratio

121. Ariel, B., Englefield, A., and Denley, J. 2019. 'Heard it through the grapevine: randomized controlled trial on the direct and vicarious effects of preventative specific deterrence initiatives in criminal networks'. *Journal of Criminal Law and Criminology*, 109:4. pp819-868.
122. See Brewer, R., Maimon, D., de Vel-Palumbo, M., Hutchings, A., Holt, T., and Goldsmith, A. 'Restorative Justice' in Brewer, R., Maimon, D., de Vel-Palumbo, M., Hutchings, A., Holt, T., and Goldsmith, A. 2019. *Cybercrime Prevention: Theory and Applications*. London: Palgrave *Cybercrime Prevention: Theory and Applications*. London: Palgrave. n.117

between police resources for fraud and for other crimes (especially other crimes for gain) is glaringly obvious and reflects an era in which recorded (and probably real) fraud was a much smaller percentage of crime than it is today, at least by volume of cases and demographic spread directly affected. If 'delivering justice' considerations are present for other police resource allocation, then the argument for excluding them from the policing of fraud is very weak, given the harms, public anxieties and proportion of reported crimes that frauds constitute. But we must address also the extent to which criminal justice is related to public health measures, whether for fraud or for other offences. It is in our view tenable that justice may be viewed as a value independent of crime and harm reduction, but it should not be confused with them.

Harm and rising volumes notwithstanding, there is less 'public pressure' to increase fraud resources than there is for other crimes, and the critiques of fraud and digital policing by HMICFRS are also strident for other areas of policing, including domestic and sexual violence. There is a prima facie need for more forensic accountants to assist policing: except for the Serious Fraud Office, we are informed that there is one in-house police forensic accountant in England & Wales and one in Scotland, compared with over 600 working for the FBI alone. It is implausible that American frauds are so much more complicated than our own, or that the top slice thereof need so much less expert help here than in North America! However, there needs to be less mystique about many other areas of fraud. The capabilities and competencies of 'ordinary' police outside Economic Crime Units need to be enhanced to educate them how to deal with far less complex frauds which may be within their remit and which do not require the lengthy investigations for which uniformed police and local detectives do not have the space. E-frauds are not going to go away, and there is a need for investigative upskilling at every level.

The challenges will be greater if reporting fraud is made compulsory (though the label of 'fraud' is not as obvious beyond volume frauds as some consider it to be).[123] Especially for more complicated frauds, there is a financial and time opportunity cost for making reports, and if such compulsory reports do not lead to positive interventions (whether criminal justice or other outcomes), then organisational victims may protest about costly and pointless regulation as some do currently about the extension of Anti-Money Laundering regulation and may do in the future about compulsory rapid reporting of corporate data breaches. Merger of economic crime units from different police and non-police departments recommended by the Treasury Committee needs to be considered in the context of different institutional data access, long chains of priority setting and decision-making, large differences in organisational culture and powers, and not least its impact on fraud in the regions.

Drew and Farrell[124] found that potential cyber fraud victims have a reasonably accurate understanding of their cyber fraud victimization risk. Those in the high risk victimization group perceived they were at greater risk compared to those in the low victimization risk group. This is interesting, given that research on other crime types has often found that individuals do not hold accurate perceptions of risk and tend to overestimate their level of risk relative to actual risk. US research found that programme dissemination and fraud prevention education efforts are most likely to be successful with individuals who are more educated, manage their finances more effectively, use the Internet, and shop online. Fraud targeting and victimization did not appear to motivate individuals to seek out information or assistance with fraud prevention, except where they had been targeted the previous year: so being a victim and recognising yourself as a victim of fraud may represent a 'teachable moment' for a range of people. We are sceptical about the validity of cross-cultural transfer of US findings a decade ago, but the way the fraud risks identified in our West Midlands analysis varied by gender and ethnicity suggest that when planning fraud and cybercrime prevention (Protect and Prepare) information, careful attention should be paid to the sorts of media that people of different demographics use.

123. Goldstraw-White, J. and Gill, M. 2021. *Mandatory Reporting of Fraud*. London: Fraud Advisory Panel. During the decades that we have researched fraud, the dismissal by the police of fraud allegations as 'civil matters' has been and remained commonplace, closing off cases in which there is often a theoretical overlap between the civil and the criminal.
124. Drew, J. M., and Farrell, L. 2018. 'Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs'. *Police Practice and Research*. 19:6. pp537-549.

Identified issues can generate resources for interventions. Let us take the frauds on the taxpayer generated by the business loans schemes as an example. The police were refused extra funding to investigate these frauds (and others attributable to the Covid-19 pandemic),[125] so they fall to be pursued – if at all - by HMRC and other government investigators (e.g., at BEIS), a retro approach much criticised by the National Audit Office,[126] which was deeply unimpressed by the amount of effort put into fraud prevention at source. Likewise, criminal attacks on Universal Credit, for which extra resource has been given to DWP by HMG.[127] To the extent that some of these tax and/or benefit fraudsters were connected to Organised Crime Groups, they might still attract the limited resources of the West Midlands and other ROCUs because of the social threats posed by those criminal actors. We are not attracted by the idea that all financial losses from fraud should be viewed independent of affordability by the individual or organisational victims; we do not agree (and no one has explicitly proposed) that these government loans frauds should attract scarce policing resource simply because they are the largest. However, the issue does highlight the importance of balancing 'sorts of victim' via differential victim impacts (on which better evidence is needed).

On the other hand, whatever the symbolic importance of criminal law, a law enforcement-led – especially not an enforcement-only - response is not always a feasible or better option. We have argued elsewhere that even if a significant organised crime or cybercrime involvement may be assumed and a 'reasonable' amount of extra resources was available – a challenge given the scarcity of skills at present - this would not solve a large proportion of investigations into fraud, nor would greater investigative success alone be likely to reduce substantially the levels of such crime. Indeed, it is now conventional wisdom in law enforcement circles that we cannot prosecute our way out of cybercrime generally or fraud in particular. This is not merely an acknowledgement of their low current and foreseeable resources but a reflection of the broader but more differentiated crime and harm reduction policy narratives that the UK government has promoted for decades in both the international and domestic contexts.

For example, one strand of more effectively policing fraud is to focus on the role of cybercrime as a medium for fraud offences through Protect and Prepare measures, though the police and Trading Standards are constrained from recommending particular products, and they may not possess specific skills for the high end fraud or cyber risks. The police.uk website refers users to GetSafeOnline and to CyberAware, but the only other specific fraud advice there is on Hajj fraud. Of course, there is a plethora of advice from different agencies and from the FCA as well as from AF and from the private sector – and post-victim reporting, on Action Fraud phone lines and from NFIB/the police after reporting - but this limited presence on police.uk looks strange. Another is whether the police take on cybercrime roles where the objectives are less about preventing and investigating financial loss than deterring those primarily involved in business disruption, and so on, thus securing business continuity and delivery and supplementing in-house security arrangements. The National Cyber Security Centre (NCSC) and its business networks might be better placed for such specialist advice.

Moreover, such measures may not solve or even mitigate the problems they are supposed to. Another strand for consideration is how far the police can investigate economic cybercrimes that have international dimensions where suspects are out of practical reach: indeed, an early decision on this could save scarce resources being wasted (though there would remain issues of victim satisfaction and care, which may not be part of a public health approach unless improved welfare can be scientifically demonstrated). Even where police interventions can arrest offenders and disrupt cybercrime markets, or the NCSC or a private/third

125. Levi, M., and Smith, R. G. 2021. *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Research Report No19. Canberra: Australian Institute of Criminology (at https://www.aic.gov.au/publications/rr/rr19); Levi, M., and Smith, R. G. 2021. 'Fraud and pandemics'. *Journal of Financial Crime*, http://dx.doi.org/10.1108/JFC-06-2021-0137; Levi, M. 2021. 'Fraud, Pandemics and Policing Responses'. *European Law Enforcement Research Bulletin*, (SCE 5). Retrieved from https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/486.

126. National Audit Office. 2021. The Bounce Back Loan Scheme: an update. HC 861. London: National Audit Office. See also National Audit Office. 2022. Progress combatting fraud; and Managing tax compliance following the pandemic.

127.. "HM Revenue and Customs is set to spend just £155million over the next two years on clawing back the estimated £5.8billion lost through the Covid support schemes it administered. The Department for Work and Pensions, in contrast, has been handed £510million to tackle the Covid-related rise in benefits fraud, estimated at £3.4billion". 'Hunt down the Covid fraudsters', *Mail OnLine* 29 December 2021 (Accessed 31 December 2021).

sector body takes down websites, their disruptive effects can be short term.[128] The NCSC has become increasingly active in this space:

- Handling 777 incidents in 2021 – a rise from 723 in 2020 and an average of 643 since launching in 2016
- 6.5 million public reports of malicious content to the Suspicious Email Reporting Service 2021-22 - up from 5.4 million the previous year – leading to the removal of more than 62,000 scam URLs 2021-22
- Engagement with around 5,000 organisations providing an essential service during the pandemic, from well-known brands through to small businesses
- Issued guidance and threat assessments to over 80 companies and 14 universities
- **The Active Cyber Defence programme** took down 2.1 million cyber-enabled commodity campaigns in 2021-22 (slightly fewer than the previous year, when it dealt with 442 phishing campaigns using NHS branding, and 80 illegitimate NHS apps hosted and available to download outside of official app stores)[129]; and may have had an impact on the number of fake UK government phishing scams, which decreased from 13,000 to 6,000 2021-22. a

Altogether, more than 2.7 million scam campaigns were stamped out in 2021, nearly four times more than in 2020. The rise reflects the expansion of NCSC services to take down additional malicious online content, such as fake celebrity endorsement scams, rather than an increase in scams overall. The work adds to suspicious emails, texts and websites reported by the public. The NCSC removed more than 1,400 NHS-themed phishing campaigns in 2021 – an 11-fold increase on 2020 – as scammers tried to trick people with fake messages about the vaccine rollout and certificates.[130] By the end of August 2022, the number of reports (since April 2020) had risen to 13.7m, while the number of scam URL addresses taken down, that were previously unknown to UK authorities, had risen to 174,000.[131] Thus, the dividing line between cybersecurity enhancement and fraud prevention has increasingly blurred.

Caring for victims needs to be considered carefully as a component of public health approaches. It is part of fraud reduction only if it leads to lower future repeat victimisation risks. However, it can be part of harm reduction even if it does not reduce repeat victimisation, provided that the evidence shows that people feel better as a result of defined interventions. Victim care has recently been extended to fraud, after earlier decades of the victims' movement in which organisations such as Victim Support assumed that fraud victims were not appropriate or priority recipients of intervention.[132] The National Economic Crime Victim Care Unit, which looks after what it interprets as vulnerable victims, is available in at least 20 police forces and in principle covers 52% of all cases reported to AF. In the year to April 2022, it supported 6,691 fraud victims.'

However, given the numbers of fraud victims that are theoretically eligible for care, it is obvious that proportionately few will receive much care in practice from the police or from the third sector. Attractive though the provision is, and though it is possible that a single conversation will help a lot, little evidence is yet available of its impact, and the term 'vulnerability' would benefit from more careful exploration for consistency and underlying evidence, to ensure that its beneficiaries are not merely stereotypes of people the agencies have identified as most deserving and/or as most likely to respond positively to offers of help.

We are aware from our previous research and from this study that developing a public health approach may propose a very differentiated response, ranging from an emphasis on Pursue where the serious organised crime or multiple/repeat victimisation dimension is evidenced and resources are available, to Protect and Prevent roles where the police take a necessary but secondary function – though we need to be clear about who, if anyone, will actually carry these roles out if the police do not do so, and how competent they are to offer advice. This may include roles for local police forces at two levels.

128. Décary-Hétu, D., & Giommoni, L. 2017. 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous'. *Crime, Law and Social Change*. 67:1. pp55-75; Bergeron, A., Décary-Hétu, D., and Giommoni, L. 2020. 'Preliminary findings of the impact of COVID-19 on drugs crypto markets'. *International Journal of Drug Policy*. 83. (accessible at: **https://doi.org/10.1016/j.drugpo.2020.102870**).
129. National Cyber Security Centre. 2021. *Annual Review*. London: National Cyber Security Centre.
130. See **https://www.ncsc.gov.uk/files/**ACD-The-Fifth-Year-full-report.pdf for more detailed analysis.
131. National Cyber Security Centre. 2022. *Annual Review*. London: National Cyber Security Centre.
132. Levi, M. and Pithouse, A. 1992. 'Victims of fraud' in Downes, D (ed.) *Unravelling Criminal Justice*. London: Macmillan.

First, they have access to the AF and NFIB data and – if they are given time to review the information - can provide significant data on risk and threats, by type, community and harm. Second, they may provide victim support, local initiatives driven by local priorities and NFIB (perhaps supplemented by those from other agencies) risk profiles, and delivery of locally tailored prevention campaigns, community engagement, championing prevention in force (e.g., all officers and staff with victim contact) and collaboration with local victim support services. This could also include suggestions that victims seek psychological help via their GPs if they find themselves distressed, though such psychological support services (and GPs) are currently and historically highly stretched.

Beyond that, we are minded to assume that the police will play a supplementary role in the Protect and Prevent functions, with the Office of the Police and Crime Commissioner looking to run or support campaigns in favour of specific protect and prevent requirements to ensure a general basic level of awareness through other organisations. Such an approach may be essential to allow the police, as trusted guardians, to offer additional guidance on protective measures against fraud and fraud-enabled cybercrime for business and individuals where the data indicates the added value thereof. The banks and government have been actively involved in Take Five and other warnings on TV, in the press, and in apps: little published evidence exists of the short term or longer impact of these information campaigns on the incidence, prevalence or seriousness of the frauds at which they are aimed. We do not doubt that these are good things to do, but it is unrealistic to expect them to be totally proof against the social engineering skills of fraudsters, which have only to be good enough to get victims to suspend their disbelief.[133] These correspond to the community levels of intervention.

Sometimes, there may be overlap between the Ps in control efforts. Thus, National Trading Standards state that its current priorities are doorstep crime and cold calling, mass marketing scams, lettings, energy related fraud, intellectual property, other fair trading issues, used cars, tobacco products and estate agents work.[134] [135]

Local Trading Standards (TS) may differ from this national picture, and the national MESH initiative may stop if it does not receive ongoing funding. The geographical units for liaison between trading standards, municipalities and police are quite large, and need to be supplemented by more organic local relationships. In short, the embedding of national-level initiatives such as these will need to take account of variations in geographic boundaries between police and Trading Standards and the ongoing need to convince local authorities of the merits of TS work, as Councils are continually squeezed by their statutory duties in a difficult economic climate and may be tempted to marginalise non-statutory activities. Joint working will need to take account of differential legislation, powers and priorities, and the integrity of council data protection systems will be a growing problem as TS information sharing with the police increases.

7.7 SUMMARY

Given the levels of fraud, and the current mechanisms for awareness, such interventions will need to be supplemented by developing a structured, coordinated, and continuing outreach programme by trusted (and trustworthy) persons. Peer influence and community level bodies seem particularly well placed to perform this function and it is better that such bodies proactively seek out or arrange face-to-face sessions with representative organisations – Women's Institutes, senior citizen groups, etc. - rather than rely on vulnerable or poorly-informed individuals to get safety advice from the internet. Older people may anyway prefer leaflets and printed materials.

We would argue that adapting or developing a public health approach is relevant and could add value to fraud responses. One difference between public health approaches to violence and those to fraud is that violence normally requires physical co-presence in ways that much fraud does not, making fraud an even bigger challenge. The amount of public investment in experimental research also needs to be factored in, though Randomised Control Trials required a radical shift from conventional observational medicine also. We consider that the conceptual thinking behind a Public Health approach will require a significant but essential shift to prevention. It will expect that organisations other than the police will take up primary responsibility on a coordinated and resourced basis

133. 'TSB refused to refund me after I was scammed, despite its fraud refund guarantee', *The Telegraph,* 3 January 2022. There are numerous other media-reported cases along similar lines.
134. Our Priorities - National Trading Standards. https://www.nationaltradingstandards.uk/site_assets/files/National%20Trading%20Standards%202020%20-%202021%20Annual%20Report.pdf.
135. Annual Report 2021-22, National Trading Standards. https://www.nationaltradingstandards.uk/site_assets/files/21-22%20annual%20report.pdf.

for encouraging people to use the internet safely and avoid dangerous activities. This will focus more on protecting the victims than on discouraging potential offenders and 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) that may tempt some into mistakenly thinking of fraud prevention as a one-off effort - a feasible approach would be to warn people about the dangers and to try and ensure that potential victims mentally register their own situation as an example of a scam or risk about which they are aware. Awareness alone is not sufficient.

Given the incidence and prevalence of frauds discussed in this report, we consider that adapting or developing a public health approach to handling them is long overdue. Further analysis and assessment of fraud data relating to the West Midlands Police (WMP) Area may be needed to make a more informed view of the added-value of such an approach and to make initial recommendations that:

- Look behind an issue or problem or illness to understand what is driving it;
- Focus on prevention;
- Propose initiatives that are reflect the three levels of intervention, and that designed, delivered and tailored to be as effective as possible;
- Propose partnerships and coordination as central because the breadth of population need requires response (intervention) across many disciplines and services.

We consider that adapting or developing a public health approach offers a fresh approach to addressing a range of frauds, and one that allows the police to focus on where their competences and techniques are best deployed. Our perspective on a public health approach may differ from that taken within a health or violence context. Exactly which interventions are best applied to what types of fraud by what mechanisms, and how their effectiveness may be realistically assessed will depend on what data we can access and what the data tell us, and the validity of fraud data should remain continually under challenge. There also needs to be a willingness to experiment, and the resource to enable this and to open changes to independent scrutiny. This does not mean that 'business as usual' will be jettisoned, but it does mean that we accept that current approaches are not just something to be added to by more financial and staffing resources and by an improved centralised intelligence function but by a range of different approaches if we are to make more than simply a symbolic impact on the different forms of fraud that have emerged and that will continue to mutate in our midst.

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