Security Journal (2025) 38:8
https://doi.org/10.1057/s41284-024-00454-0

ORIGINAL ARTICLE

Will the future policing of fraud be 'a fundamental shift in our approach to tackling fraud' or largely more of the same? Reviewing the 2023 UK fraud strategy through evidence on the ground

Alan Doig[1] · **Michael Levi**[1] · **Jodie Luker**[1]

Accepted: 16 September 2024

Abstract

In 2023, the UK government issued a national Fraud Strategy in response to concernsover increases in reported fraud and the low levels of law enforcement resourceavailable to investigate cases. The Strategy was announced as a fundamental shift inhow the government intended to respond to frauds and attempted frauds againstindividuals. The article focusses on the evidence base that may be assumed tounderpin and shape any strategy by assessing and analysing the data what wouldhave been available at the time the Strategy was drafted.The article argues that the Strategy has not taken any time to explore paststrategies and any lessons to be learned and nor did it appear to substantivelyaccessed, used, analysed and interpreted the available data, and nor used that data asan evidence base to develop an approach will have to be strategic, prioritised andinnovative. The article concludes that, in strategic terms, the Strategy may be unlikelyto achieve its objectives.

Keywords Fraud · United Kingdom · Policing · Central government · National strategy

✉ Alan Doig
doigdurham@msn.com

Michael Levi
Levi@cardiff.ac.uk

Jodie Luker
LukerJR@cardiff.ac.uk

[1] School of Social Sciences, Cardiff University, Cardiff CF10 3AT, Wales

Published online: 04 December 2024

Introduction: the fraud pandemic and an evidence-based strategic response?

In September 2023, the UK House of Commons Home Affairs Committee began an inquiry into fraud.[1] Quoting figures from the 2023 National Fraud Strategy on the prevalence of fraud and perceived inadequacy of the police resource devoted to it, its remit was to examine the UK's response to fraud and the impact of serious fraud offences and fraud against the public sector; to understand what the Government are doing to combat the scale of fraud in the UK; and to examine the effectiveness of the Government's counter-fraud policies, including the fraud strategy and the economic crime plan. Its question in relation to the strategy was: whether the government's recently published Fraud Strategy does enough to combat fraud? Launched less than six months earlier the 2023 Fraud Strategy explicitly stated that 'fraud poses a significant threat to the people, prosperity, and security of the UK. It is by far the most common crime and now accounts for over 40% of all offences in England and Wales'. To combat this, it intended to 'tackle fraudsters head on and cut fraud by 10%, protecting the British people's hard-earned cash from criminals and putting more fraudsters behind bars' (HM Government 2023a: 3[2]).

From being an always marginal crime issue in the public arena, frauds[3]—or more accurately, public-facing 'volume' frauds—have become a mainstream crime. In 2023, the Social Market Foundation (2023: 4) stated that 'fraud has now reached epidemic scale, yet the response from the authorities, as well as the private sector, has been consistently insufficient in the face of the scale and complexity of the problem. The upshot of the inadequate efforts so far has been increasing amounts of financial, psychological and social harm to a growing proportion of the UK population'. In the same year, Button et al (2023a: 8) argued that 'the threat forces in favour of fraud currently overwhelm the safeguard forces. The array of threat forces has been hugely amplified by the disruptive impact of new technologies… Indifference is the essential cause of the weakness of the safeguard forces: an indifferent public,

[1] The then Home Secretary in her Foreword to the National Strategy (https://www.gov.uk/government/publications/fraud-strategy).

[2] The reference to cutting fraud by '10%' was explained as follows: 'based on the latest figures available from the Office of National Statistics (ONS), in the year to December 2022 there were 3.7 million frauds estimated. Our ambition is to cut fraud by 10% from 2019 levels, down to 3.33 million frauds by the end of this Parliament. We will prevent over 300,000 frauds through Pursue interventions alone' (HM Government 2023a: 50).

[3] This article prefers 'frauds' to 'fraud' because the application of a single homogenous term onto an eclectic jumble of criminal activities fails to recognise the variable impacts of and responses to a very broad range and variety of fraud offences. It defines frauds as actions or activities (including attempts) intended to achieve financial loss or potential loss by individual and organisational victims, online and off-line, through a variety of unlawful means, or unlawful exploitation of lawful means, including abuse of trust, deception, misappropriation, or misrepresentation. Our construct is narrower than the notion of 'economic crime' in the UK Government's 2019–2022 Economic Crime Plan, which 'defines' it as a broader 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.

marginal interests within law enforcement, irresponsible organisations, and dismissive politicians'. Such concerns are reflected and repeated in critical reports from parliamentary committees, as well as from the police inspectorate (HM Inspectorate of Constabulary, Fire and Rescue Services [HMICFRS; formerly HM Inspectorate of Constabulary [HMIC]), the Police Foundation and other bodies. Noting the escalating number of fraud cases and how the UK (or, more precisely, how England and Wales) deals with frauds, the range of reports and articles indicate a clear consensus on the unfitness for purpose of a reliance primarily on the police PURSUE function[4] for frauds high and low (see, for example: National Audit Office 2022; Victims Commissioner (Poppleton et al 2021); House of Lords Fraud Act 2006 and Digital Fraud Committee 2022; Treasury Committee 2022; Committee of Public Accounts 2023a; 2023b; Royal United Services Institute 2022; Social Market Foundation 2022; Spotlight on Corruption 2022; Skidmore and Aitkenhead 2023).

Reflecting these critiques, the government's response was the 2023 UK Government's Fraud Strategy (the 'National Strategy'; the City of London Police also issued a national policing strategy for fraud, economic and cyber crime in the same year). This reported that 'the volume of fraud, its capacity to undermine public confidence in the rule of law, and its potential negative effect on the UK's financial reputation, means it should be considered a national security threat…(and that) the criminal justice system must ramp up the focus it gives to fraud' (HM Government 2023a: 9,14). It identified the main drivers for increased cases and losses as the internationalisation of fraud, use of new technologies and the ubiquity of the Internet. The proposed mixed public and private responses involve five main areas: addressing cold-calling and scam texts; revamping Action Fraud and more intelligence-sharing; improving financial reimbursement and prevention; improving the law enforcement response and more convictions; and encouraging internet companies to protect users and consumers. Delivery would be achieved through multiple agencies and sectors, overseen by the Economic Crime Strategic Board.[5]

The expressed need for a strategic approach to fraud is not new: the Fraud Review (2006: 6) noted that 'the majority of people consulted during the review felt that the government must formulate a national strategy for dealing with fraud. The strategy should take a 'holistic' approach, focussing efforts and resources where they are likely to be most effective rather than most attention grabbing, and focussing on the causes of fraud as well as dealing with the effects'. In so doing, however, it also underlined in its Final report a central prerequisite to taking a strategic approach: 'measurement is fundamental; without better information about the scale and nature

[4] Though apparently abandoned in the 2023 Serious and Organised Crime Strategy, the 4 Ps (PURSUE; PREVENT; PROTECT; and PREPARE) had been used to define the four dimensions for law enforcement responses: investigating, prosecuting and disrupting suspects (PURSUE); preventing people from engaging in criminality (PREVENT); increasing protection against criminality (PROTECT); and reducing the impact of this criminality where it takes place (PREPARE).

[5] The Board is a Home Office-sponsored committee comprising senior government, law enforcement, regulatory, prosecutorial and financial services representatives which is responsible for the Economic Crime Plan whose second iteration (2023–2026) is intended to address: a reduction of money laundering and recovery of more criminal assets, combating kleptocracy and driving down sanctions evasion, and cutting fraud.

of fraud it will be impossible to develop a sensible national strategy for dealing with fraud' (Fraud Review 2006: 5).[6]

We consider that this emphasis on the analysis of crime data, patterns and trends extant at the time of the drafting of the National Strategy is not only a standard approach to ensuring that any fraud strategy is an evidenced response to identified issues but one which reflects the more general criminal justice approach: 'decisions about which crimes or offenders to focus on appear to be more strongly influenced by explicit policies, strategies or 'policing plans' – themselves ostensibly the result of careful analyses of crime patterns and trends, as well as taking account of the priorities of central and local government, other agencies and local communities' (Levi and Maguire 2012: 195).

This article asks a number of questions: what was the scale and nature of frauds of different types at the time the National Strategy was drafted? what would an analysis of available data have said about potential responses? Would such an analysis have provided a defensible basis for developing a strategy? The publicly available data are supplemented by empirical data from one large, mostly urban metropolitan police area[7] which would have been available to those drafting the National Strategy. The article considers how profound a change is the National Strategy likely to be—how fundamental a shift in the approach to tackling fraud does it represent and will it, as the UK House of Commons Home Affairs Committee asked, do enough to combat fraud?

Article focus and framework

This article recognises that frauds impact across public, private and third sectors and that many frauds, in terms of volume and value, are investigated—often with substantial resources—within those sectors, and outside the police framework.[8] However, this article focusses only on data relating to those frauds for which the National Strategy is the proposed response, with an emphasis on public-facing 'volume'

[6] The Fraud Review resulted in the first national fraud strategy being issued in 2008 by the National Fraud Authority (NFA). In 2011, the NFA issued an overarching national strategy review before being unexpectedly abolished in 2013 and its various responsibilities distributed among a number of other bodies (see Levi and Doig 2019).

[7] It is recognised that, in a number of areas, the quality and relevance of data have improved significantly but we are interested in the data available to those responsible for drafting the National Strategy.

[8] For example, in 2023, HMRC issued its final statement (https://www.gov.uk/government/publications/measuring-error-and-fraud-in-the-covid-19-schemes) on the three COVID-19 support schemes it administered; the Coronavirus Job Retention Scheme, the Self-Employment Income Support Scheme, and Eat Out to Help Out. It estimated that across the full lifecycle of the three financial support schemes up to 2022, the total value of error and fraud was £3.3-£7.3 billion, with a most likely estimate of £5.0 billion. A year earlier, in October 2022, the House of Commons Committee on Public Accounts (2022: 14) reported that the Department for Work and Pensions had suffered £6.5 billion fraud losses but that Department had planned an increase in frontline counter-fraud staff to 9,500 full-time equivalents by July 2022.

frauds: individual victims whose responses are noted by the Crime Surveys of England and Wales (CSEW) and/or who report to and through Action Fraud.[9]

The methodological framework used to address the questions is the use of literature searches, desk reviews and a case study approach, including quantitative data analysis. The methods were chosen to reflect good practice context: 'numerous techniques for data collection, analysis, and interpretation abound in public management, but three special ones are literature review, interview, and document analysis' (Osifo 2015: 7). The document analysis comprised desk reviews of official and other documentation relating to the policy and practitioner approach to fraud relating to, and subsequent to, the 2006 government review as well as public domain sources and academic publications.

The supplementary data reflect a case study approach because it adds to the other methods by empirically inquiring into 'a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident' (Yin 2009: 18), in order to 'develop concepts, insights, and understandings from patterns they see in their collected data…' (McNabb 2015: xix). The data from the case study are intended to add nuance and a deeper understanding of the wider publicly available data. It comes from a wider practitioner project (the 'project') for the West Midlands Office of the Police and Crime Commissioner.[10] The data were twofold: all frauds reported to Action Fraud for the West Midlands Police (WMP) area, and those data analysed and disseminated to WMP by the National Fraud Intelligence Bureau (NFIB). All frauds are allocated to 50 fraud categories pre-determined by the NFIB at that time. The first dataset involved over 20,000 recorded cases reported during the period May 2020 to July 2021; the second concerned over 1000 cases between April 2020 and March 2021. This has limitations in terms of 'the size of sample, the snapshot nature of the research, or the restriction to one geographical area of an organisation' (Saunders et al. 2009: 538).

The data analysis involved the following variables[11] embedded in NFIB-determined datasets: Ethnicity, Fraud Loss, Victim Type, Repeat Victimisation, Fraud Type, Age and Postcode. To ensure consistency and accuracy of analysis, the

[9] Recorded by the National Fraud Intelligence Bureau (NFIB) via direct reporting to Action Fraud or credit and debit card and other financial losses reported via Cifas (a not-for-profit fraud prevention membership organisation, whose members are primarily financial services and corporate businesses) and UK Finance (a trade association for the UK banking and financial services sector, representing over 300 firms in the UK providing credit, banking, markets and payment-related services). In estimating the cost of fraud, the National Strategy only estimates the impact of fraud against individuals in England and Wales because, 'due to data constraints, the cost of fraud offences committed against businesses and the public sector are out of scope of this estimate' [HM Government 2023a: 56]. However, a survey of cost of fraud against business is in progress.

[10] https://www.westmidlands-pcc.gov.uk/fraud/. The authors would like to thank the West Midlands Office of the Police and Crime Commissioner for use and analysis of the data for academic research purposes.

[11] The data utilised NFIB categorisation: Ethnicity (Asian, Black, Mixed, Other Ethnic Group, White Other, White); reported fraud loss (£); Individual or Organisation; Repeat Victimisation (Prior Victim of Fraud or not); Fraud Type (NFIB categories); Age categories (< 24, 25–49, 50–69 and 70 +); West Midlands postcodes (5 postcodes).

variables were recoded across waves and appended together. The data were prepared for analysis using a combination of Microsoft Excel and the statistical software package STATA (StataBE Version 17). It distinguishes between mean and median loss, generally opting for displaying the median losses by not including outlier losses which have a disproportionate effect on averages (though acknowledging that large verifiable losses may be important as a trigger for crime investigation and loss reduction, and sometimes for social harm). The case study was supplemented by unstructured interviews with representatives of the police, Trading Standards and other relevant agencies as part of the project, using flexible conversations that allow questions to emerge through the interviewees' discussions and provide a better appreciation of their perspectives and their roles towards developing an understanding of what types of fraud cases are also undertaken by other agencies (see Zhang and Wildemuth 2017: 239–247).

The article is structured as follows: publicly available data on frauds, their volume and costs from 2019 to 2022 at the point when the National Strategy was in preparation[12]; the case study analysis of the fraud reports facing one police force at that time; and what the two data sets say to the authors and readers about the National Strategy as a fundamental shift in approach and whether it does enough to combat fraud?

Fraud data and the 2023 National Strategy

The volume and costs of frauds

Drawing on Office of National Statistics (ONS) crime survey data at that time (Office for National Statistics 2022; the Telephone Crime Survey of England and Wales [TCSEW])—the National Strategy stated that fraud accounted for 40% of all 'crime' (over 4.4 million reports) in England and Wales. The ONS also recorded that, in the same year, reports to Action Fraud were 326,000 to which were added those reported to NFIB by Cifas—nearly 330,000—and UK Finance—just over 467,000) or less than 27% of the ONS December 2022 figure.[13] In operational terms, using Action Fraud's own data for 2020–21, NFIB disseminated just under 60,000 cases from those received by Action Fraud; of those 60% were considered amenable to the PURSUE function, or just over 3.5% of the December 2021 ONS figure (and less than 1% of the December 2022 ONS figure).

While the National Strategy does present figures on aggregate losses and 'incidents', there is very limited discussion on variations of data—such as loss sizes and the volume of 'incidents'- and what they could or would mean for investigation or additional police numbers. (Although the variations may in part come from the

[12] The authors appreciate that there are more recent data, but it would be inappropriate to use them in the framework of this article.

[13] In the previous year, the last time it published the data itself, Action Fraud's own data recorded over 400,000 reports of fraud (to which are added those reported to NFIB by Cifas – nearly 320,000 – and UK Finance – just over 143,000).

terms 'crime' and 'incident' which were used interchangeably in compiling the ONS data at that time—i.e. where the bulk may have involved attempts of which victims were aware). There was also no discussion on the reasons for the disparity with the Action Fraud figures and the levels of reporting (although an earlier 2019 CSEW survey (ONS 2019) did ask TCSEW victims why they did not then report to Action Fraud[14]) where these data should have had strategic implications as to how to rectify the under-reporting, nor on the reasons for, and implications of, the substantial attrition between ONS data, incidents reported to Action Fraud, those disseminated by the NFIB, and those disseminated that had criminal justice or other identifiable outcomes.

Using a range of data that for uniformity purposes is anchored in pre-2023 data from a range of sources, the National Strategy estimates the total 'cost' of fraud is £6.8 billion. The £3.1 billion reported financial losses (HM Government 2023a: 57) are more than Action Fraud data (£2.35 billion in 2021). Fraud losses had been subject to widely varying assessments, from the 2000 Home Office-commissioned report (NERA 2000) which argued that discovered fraud could range from £5b–£9 billion, to former National Fraud Authority (NFA) annual fraud indicators which rose from £30 billion in 2010 to £73 billion in 2012. In 2021 the House of Commons Library claimed that fraud could cost the UK over £137 billion a year.[15]The more grounded National Strategy figures comprised estimated losses of over £3 billion from the TCSEW survey for the year ending March 2020; the rest are assessments and extrapolations associated with prevention, loss of productivity by victims, health treatments, criminal justice processes, and so on, in accordance with the well-established Home Office cost of crime model. The biggest single 'cost' outside reported losses is a Quality Adjusted Life Years (QALY) approach applied to monetise the emotional impacts of anxiety, depression, and fear on victims at £1.3 billion; police costs in 'response to crime' were assessed at £0.2 billion.

Victims

The National Strategy wants to increase victim support, including ensuring vulnerable victims receiving more tailored support at a local level. It notes from the TCSEW that 18% of those victimised became victims more than once and, according to TCSEW 'calculations', account for 35% of all fraud. Victim care has recently been extended to fraud by a range of bodies, after earlier decades of the victims' movement in which organisations such as Victim Support *assumed* that

[14] In 2019, the CSEW survey asked why respondents did not then report to Action Fraud. 85% of respondents stated the main reasons for not reporting to Action Fraud were: reported to financial authorities (40%); thought incident would be reported by another authority (23%); private matter/dealt with matter themselves (12%); and too trivial/not worth reporting (10%). Such information should also have had implications for any strategy as to how to rectify the under-reporting.

[15] 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: 5), the cost was mentioned as £4.7 billion annually, a figure taken from the first HMG Economic Crime Plan which was published in 2019 and which had taken that figure from a 2018 Home Office-published report which in turn had taken the figure from a 2015–16 CSEW report (Heeks et al 2018: 17).

fraud victims were not appropriate or certainly not priority recipients of intervention (see Levi and Pithouse 1992). The National Economic Crime Victim Care Unit (NECVCU), which looks after what it interprets as vulnerable victims, is now available across police forces and in principle covers nearly all cases reported to Action Fraud (although the term 'covers' may range from personal contact to the mailing of leaflets to such victims with general prevention advice and the names of potential support organisations).

In practical terms, the National Strategy did not demonstrate how it calculated responses in terms of likely demand. 'Bolstering victim support' could suggest, using the 18% repeat victim figure, responses capable to managing an annual pool of those likely to need support from Action Fraud of some 60,000, or nearly 800,000 using TCSEW figures. Research using crime survey data (Poppleton et al 2021) 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), 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', 'medium-vulnerability victims', and 'low-vulnerability victims'. Research[16] suggests there were around 700,000 high-vulnerability victims in 2018/19, with victims likely to have experienced financial loss, with property or money taken, who were likely to say they had been affected a lot and to have experienced severe or multiple emotional reactions, including anxiety or depression.

Certainly, in failing to map the numbers involved against available resources, the National Strategy was not in a position to determine what response should be in place if the current provision could be extended for large increases in victims, which bodies would triage victims to ensure the right support, who will provide it and how would it be funded, particularly if sustained or non-policing support is needed. On the basis of available data, a victim's contact with the police is often limited to a phone call to outsourced civilians at Action Fraud, leaving ambiguity over where the responsibilities lie for any follow-up that may be required, whether through the NECVCU, local police, or any other non-police organisation, such as the local authority. All police forces are notified of fraud victims in their jurisdiction (Action Fraud data show a fourfold increase to over 9000 'Protect' cases from its 2019–20 to its 2020–21 figures), but a number of forces had at that time 'no structures or systems in place for monitoring these or delivering additional support' and therefore, most victims would not be entered onto a local crime database (see Skidmore et al. 2022: 32).

Policing fraud

The National Strategy argued that 'victims must know that the police will do something about their crime', though fraud 'receives less than 1% of police resource' (HM

[16] See Levi, M. *The Impacts of Frauds and Responses to Them.* Written evidence to the House of Commons Home Affairs Committee, published January 2024 (https://committees.parliament.uk/work/7913/fraud/publications/written-evidence/?page=2).

Government 2023a: 1). 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/financial intelligence officers are also allocated within other major crime units): this constituted 0.64% of total staff. The National Strategy did not provide any breakdown of the staffing resource dedicated to fraud, including information on internal distribution of cases within police forces and between police forces, although the allocation of police staffing resources-civilian and warranted—to fraud has long been the subject of concern both because of force priorities and competing agendas. In 2021, HMICFRS returned to an earlier report (HMICFRS 2019) to note that there were 'too few examples of the police and other agencies coming together to prevent and protect the public from fraud; there are far too few officers working on it; there are far too few investigations into it; and there are far too few criminals brought to justice. All this leads to far too few victims receiving the service, and the justice, they want and are entitled to expect' (HMICFRS 2021: 27).

The National Strategy claimed that '70% of fraud either originates abroad or has an international element' (HM Government 2023a: 11). While this may be true overall, available data pointed to the importance of disaggregating such a picture because in relation to 19 NFIB categories of fraud—or nearly 17,000 cases in 2021—both the perpetrators and the offence were, according to an NFIB memo in February 2022, solely based in the UK.[17] Although such cases were more likely to be investigated—or could be investigated—by UK law enforcement, the National Strategy did not provide an analysis of what the optimum number of officers should be and for what purposes across UK police forces. Further, it did not discuss the criteria against which cases could or should be investigated. Police forces have often used a crude numeric value below which cases would not be pursued, and which does not formally take account of impact on victims (admittedly, not an easy task): in 2000, the average case value was £100,000 (£177,000 at 2024 prices) on a spectrum of £46,000-£2.3 million being dealt with by some 700 officers who finished nearly 50% of cases within a 12-month period (Doig et al 2001: 100).

Without such an analysis, such a crude filter may continue to apply to most cases and, in any event, most cases reported to Action Fraud would not be investigated. There were—and is—data on the mean or median costs of fraud by victim or offence. According to the National Strategy, only 0.5% of CSEW incidents (less than 20,000) had a value of over £10,000. The TCSEW survey for the year ending March 2020 also noted that 26% of cases involved no loss and, of those that did, 76% involved losses of less than £500 and the median loss was £150. The *average* loss for the 875,000 cases sent to NFIB for potential dissemination to police forces was just over £2600 (or an average loss of some £7,500 for those who report directly to Action Fraud). It is unknown what percentage of these are triaged for dissemination or receive substantial criminal investigation, as this was not within the regulatory purview.

[17] Available from an unpublished police intelligence report obtained by the Labour Party under the Freedom of Information Act and issued in December 2023.

Sanctions against offenders

Despite such issues, however, the National Strategy was explicit that 'most victims do not see justice done, and most fraudsters are not punished for their crimes' (HM Government 2023a: 22), while the 2023 policing strategy stated that 'improving the response to victims is vital'. A corollary of this is to improve success of prosecutions and/or confiscating and returning the proceeds of fraud to victims. The National Strategy did not actually say how this was to be achieved, other than a review into the challenges of investigating and prosecuting fraud, the Fraud Act 2006 and 'the entire life cycle of a fraud case'. Until such time, however, it remains unclear as to how the National Strategy could or would improve the current situation. The number of arrests has been declining over the past two decades to a sixth of what they were; as incidents and reported frauds have risen, fraud arrests have fallen in absolute terms as well as in relative terms (see Table 1). Ministry of Justice data show that in the year ending June 2021, 4406 people were sentenced for fraud, of whom a quarter (1120) 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.[18]

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 (although we note the implications of a directional shift in the law enforcement response to fraud below). As with much policing, cases in which there is strong evidence against local perpetrators will be the most cost-efficient to prosecute. In terms of judicial outcomes other than prosecution[19] and using the last publicly available Action Fraud data on referrals and outcomes for fraud, over 58,000 reported frauds were referred to police forces. Over 35,000 of these were disseminated for investigation (around 4% of reports) and some 6363 cases resulted in a judicial outcome in the same year (or a possible 11% of cases or under 1% of those reporting a fraud to Action Fraud.

Restitution

In terms of reimbursement, fraud victims can in principle be compensated in several ways: from court orders following criminal 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

[18] See Tables Q 5.2 https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2021.

[19] These may include: prosecution under an alternate offence; a caution; a record of 'taken into consideration' (which requires an admission of the offence); fine; community resolution; a decision by CPS not to prosecute; prosecution prevented (by, for example, offender ill, or victim declines to support police action); prosecution time limit expired; and so on.

awarded; and from industry schemes such as the Contingent Reimbursement Model Code 2019 bank agreement to compensate victims of Authorised Push Payments (APP).

Despite the Banking Protocol (recently under review by the Payment Systems Regulator [PSR][20]), and the National Strategy's proposal to put'reimbursement on a mandatory footing' (HM Government 2023a: 42), compensation for APP victims remains a contested space, with media allegations that some banks are not doing enough to reimburse their customers, though many readers' comments on those press articles counter that the banks should *not* be responsible for customer lack of awareness or diligence [an issue highlighted by a judicial decision that it was not the bank's responsibility to 'concern itself with the wisdom or risks of its customer's payment decisions' (Supreme Court 2023: 2)]. For all other victims, plans by the National Strategy for reimbursement remain unclear, other than considering (HM Government 2023a: 42) 'a consistent framework for repatriation of fraud funds to victims both in the UK and abroad' (the latter being an important principle that also encourages reciprocity).

The article now takes these broad issues identified in the publicly available data and seeks to explore them in more depth, and from the bottom up, in terms of data relating to a single police force.

Fraud data as a basis for fraud policy and control for the National Strategy: case study data

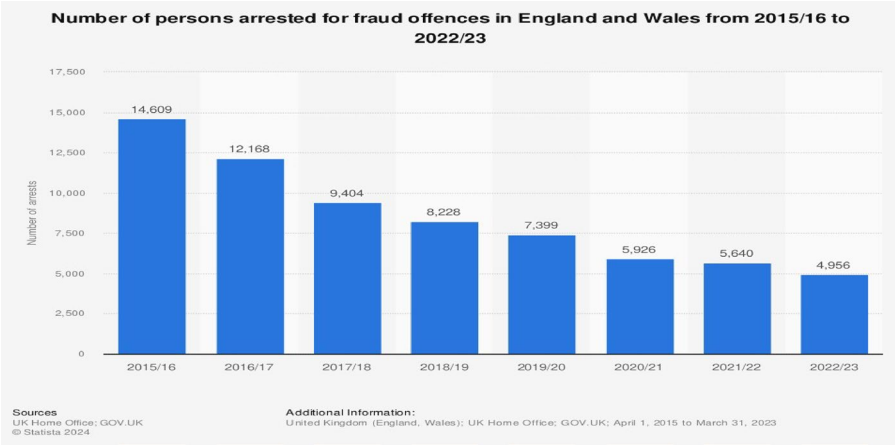
The usability of the data

The case study data derive from an Action Fraud dataset relating to the West Midlands Police force area. Fraud—cases recorded by Action Fraud—is not the largest component of recorded offences in 2021 (around 5%—or over 17,000 cases—where violence against the person and theft offences made up 70% of all cases), while 0.75% of WMP's FTE served in the Economic Crime Unit and Regional Asset Recovery team. The data set related to over 20,000 reports of fraud from May 2020 to June 2021. The project also developed another dataset of NFIB Disseminations of over 1,000 reports of fraud for investigation by the WMP between April 2020 and March 2021. Thus, approximately 5% were considered for investigation. Of these latter, fewer than 10% resulted in a judicial outcome to date—and half of those outcomes resulted in suspects being charged or summonsed—or approximately 1% of the reported frauds. No further action was taken in over three quarters of the reports, largely because of evidential issues. Just over 13% of cases were still pending. In general, therefore, The WMP picture was not significantly different from the overall national picture at that time and a deeper dive from the case study could plausibly complement the public data.

In the context of the National Strategy's intention to share and use data for fraud patterns and trends, the inadequacies of the data analysed at that time should

[20] See https://www.psr.org.uk/our-work/app-scams/.

Table 1 Decline in arrests for fraud offences



be noted. The Action Fraud data were incomplete; there were no data on gender, although there were for age and ethnicity. In some categories, the age of the respondent, ethnicity or reported value of the fraud were unrecorded or incompletely recorded (in the case study there are 5 NFIB categories with half or more entries of age missing, 17 with half or more value of loss missing, and 9 with over a third ethnicities missing). Cases were not adequately assessed; more than a quarter of reported cases were in NFIB90 (the 'None of the Above' NFIB category applied to frauds assessed but not able to be allocated to the other NFIB fraud categories at that time). This covered a very varied mix of cases, but many of them would also be suitable for inclusion in other categories. This category made it very difficult to distinguish between frauds, and victims of frauds, to understand fraud patterns and trends, and to design preventative measures.

There also needs to be attention given to the credibility or accuracy of the data. The national data suggested an average loss of under £10,000 per case compared with around £8000 in the West Midlands, but in the latter context, 61% of recorded fraud was accounted for by 17 cases (£1 million and over). These large cases represented a range of AF categories where three involved company fraud, two involved investments, three involved controlling behaviour relating to property (and one was logged at 10×the value reported in the narrative). Two of the largest reported losses raise questions about the veracity of the claim (or the ability of the Action Fraud assessment process to verify the likelihood of the level of fraud taking place), given the nature of the allegation or interpretation by the recording process (and why, since such figures skew the data, this article uses median as well as mean values).

The volume and cost of frauds

From the 50 NFIB fraud categories and over 20,000 cases reported to Action Fraud relating to the WMP area, over the 14 month period, most specified categories of fraud had few reported cases. Only 5 categories each had more than 5% of the total

of reported cases as follows: None of the Above (NFIB90)—27% of cases; Online Shopping and Auctions (NFIB3A)—24% of cases; Other Advance Fee Frauds (NFIB1H)—8% of cases; Other Consumer Non Investment Fraud (NFIB3D) 7% of cases; Cheque, Plastic Card and Online Bank Accounts [not Payment Service Provider][21] (NFIB5A)—7% of cases. Of the remaining 45 categories, only 3 had more than 500 cases reported: NFIB2E (Other Financial Investment); NFIB3E (Computer Software Service Fraud); NFIB52C (Hacking—Social Media and Email). 27 categories had fewer than 100 cases and 15 had less than 10 cases each.

The overall reported losses were £227 million; on the other hand in about a third of reported cases, there were no any reported losses as stated by the victim. Within the 5 main fraud categories by volume, the 3 highest associated losses were as follows: None of the Above (NFIB90)—15%; Online Shopping and Auctions NFIB3A)—14%; Cheque, Plastic Card and Online Bank Accounts (not PSP) (NFIB5A)—7.5%; Other Consumer Non Investment Fraud (NFIB3D)—3%. 7 other categories had similar losses, ranging from over £5 million to over £70 million but from a much smaller number of cases (under 2000 in total). Of the 27 categories with fewer than 100 cases, the total reported losses were over £16 million (or 8% of losses; with the removal of one case reported at over £14 million, the 27 categories involved over £2 million in losses, equalling 1% of reported losses).

The mean (average) loss by category emphasises the impact that a limited number of cases with high reported losses can have on the overall picture. Thus, NFIB52E (Hacking Extortion), NFIB19 (Fraud by Abuse of Position of Trust), NFIB8A (Corporate Employee Fraud), and NFIB9 (Business Trading Fraud) had mean losses in excess of £100,000. For this reason and concerns over the credibility of some of the larger reported losses, the project opted for displaying the median losses, since outlier losses appeared to have a disproportionate effect on averages (though verified large losses may be important as a trigger for crime investigation and loss reduction, and sometimes—but not always—as an indicator of social harm). Here, the value per case was significantly lower and the categories varied.

Thus, the main categories for median losses over £5000 are as follows: NFIB10 (False Accounting); NFIB14 (Fraudulent Applications for Grants from Government Funded Organisations); NFIB9 (Business Trading Fraud); NFIB8B (Corporate Procurement Fraud); NFIB8A (Corporate Employee Fraud); NFIB16B (Pension Fraud committed on Pensions); and NFIB4B (Fraudulent Applications for Grants from Charities). While it is accepted that *all* these frauds were considered by their victims to be important enough to take the trouble to report to Action Fraud, it is also clear that frauds—as opposed to 'fraud' as a collective noun—reflect a very varied spectrum within which to prioritise both responses and resources. In particular, analysis of the project data noted that the five fraud category types by volume of reported cases (73% of the 20,000 reported cases) also had significantly lower median losses,

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

ranging between £30 and up to £500 median loss per case.[22] This represents the big difference between more numerous volume frauds and rarer corporate-type frauds.

Victims

The project data reaffirm that differentiations also exist in victim demographics. Some types of frauds are more prevalent among different age groups—nearly half of lender loan (advance fee) frauds are against the 25–49 age group—while others, such as lottery scams, show an equal distribution among the 25–49, 50–69, and over 70 groups. Dating scams, like online shopping and auction frauds, are more closely associated with those between 25 and 69. But those over 70 are not vulnerable equally to *all* types of financial frauds: they were more likely to be victims of pension scams, but less likely to be victims of NFIB2B (Pyramid or Ponzi schemes) and are likely to be disproportionally represented in cases involving Computer Software Service Fraud (NFIB3E), Fraud by Abuse of Position of Trust (NFIB19), and Door to Door Sales and Bogus Traders (NFIB3C).

An analysis of ethnicity and fraud categories was affected by a significant amount of missing data for this variable. However, ethnicity correlation with susceptibility to particular types of fraud showed that NFIB6B (Insurance Broker Fraud), NFIB2E (Other Financial Investment), and NFIB3F (Ticket Fraud) are more likely to be more associated with being Asian or British Asian victims; NFIB2B (Pyramid or Ponzi Schemes) with being Black or Black British victims; NFIB3E (Computer Software Service Fraud) with White victims and NFIIB4A (Charity Fraud) with 'White Other' victims. However, the small number of cases for some fraud types should suggest caution about inferring that these ethnicities are at a *significantly* higher risk, still less that they are targeted *because* of their ethnicity.

The data show that over 40% of those reporting fraud have been fraud victims before. There were statistically significant differences, e.g. over a third of online shopping and auctions (NFIB3A) victims were repeat victims. Cases involving a large number of repeat victims are Cheque, Plastic Card and Online Bank Accounts (not PSP) fraud, Fraud by Abuse of Position of Trust, Hacking (Personal) and Door to Door Sales and Bogus Traders frauds. When matched with the two higher levels of victim vulnerability, the most likely fraud categories for large numbers of vulnerable repeat victims are Hacking (Personal), Time Shares and Holiday Club Fraud, Other Financial Investment, Dating Scams, and Hacking (Extortion). However, we are unable to clarify whether 'repeat' applies to the same type of offence, to a range of categories, to the frequency and rapidity of the victimisation, or to multiple frauds within the same fraud (such as escalating payments in a NFIB1A [Advanced Fee] fraud).

[22] By way of comparison, in the year to March 2022, the TCSEW reported that nearly 28% of victims of bank and credit account fraud suffered no loss and, of those who did, 57% had losses under £500 (i.e. 90% of respondents had losses under £500). The latter percentage was very similar for victims of consumer and retail fraud and advance fee fraud: see https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse.

When the data are aggregated by, for example, age, ethnicity and postcode, identifiable patterns of victimisation emerge. Some fraud categories were more prominent in some areas; for example, in one postcode, over 70% of pension liberation frauds affected the 25–69 group, while, in another, 60% of those 70 + were affected. The research suggested that certain frauds had repeat victimisation levels of 50% + across postcodes; NFIB19 (Fraud by Abuse of Position), NFIB3G (Retail Fraud), NFIB3C (Door to Door Sales and Bogus Traders), NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)), and NFIB8A (Corporate Employee Fraud). Other categories such as NFIB 13 (Bankruptcy and Insolvency), NFIB15 (HM Revenue and Customs Fraud (HMRC)), NFIB52A (Hacking—Server), NFIB5E (Dishonestly retaining a wrongful credit) and NFIB9 (Business Trading Fraud) also suggested high levels of repeat victimisation but with variations in levels across postcodes.

Policing fraud

A review of Disseminations data for approximately the same period showed that the NFIB sent out some 1200 reports[23] for investigation. 174 of these were transferred from other forces—which has implications not just for the length of time towards an outcome but also the willingness of the 'incoming' force to accept the referral and the 'freshness' of the investigative and evidential trail. In 14 categories, no cases were disseminated. Of the categories that were disseminated, the greatest number—reflecting more than 5% of the total number of disseminated cases—were NFIB19 (Fraud by Abuse of Position of Trust)—15.6%; NFIB2E (Other Financial Investment)—10.9%; NFIB3A (Online Shopping and Auctions)—12.6%; NFIB52C (Hacking—Social Media and Email)—8.3%; NFIB5A (Cheque, Plastic Card and Online Bank Accounts [not PSP])—7% of cases; NFIB90 (None of the Above)—7% of cases.

Of the retained disseminated cases, over 60% were not pursued on grounds of evidential difficulties. In terms of judicial or other outcomes, 36 people were charged or summoned; 22 were cautioned, 7 were subject to community resolution and 1 received PROTECT advice. In short, the case study data suggest that around 10% of reported fraud is likely to be triaged by the NFIB for dissemination and, of these, less than 5% will result in some form of positive outcome. Overall, less than 1% of all fraud reported to Action Fraud was likely to end up being investigated by the WMP.

Because of a small period of overlap between the Action Fraud data and NFIB disseminated data, and using the same criminal reference number, the project was able to track a small number of Action Fraud reports which were later included in the Disseminations data. While too small to determine specific outcomes or trends, analysis suggested that the biggest categories for potential investigation were NFIB19 (Fraud by Abuse of Position of Trust)—31% of cases; NFIB52C (Hacking—Social Media and Email)—19% of cases; and NFIB90 (None of the Above)—9% of cases. Of these, the cases involving NFIB19 (Fraud by Abuse of Position of

[23] Spreadsheet data is supplemented with hard copy intelligence about specific cases, such as links to other cases or involvement to organised crime; these were not available to the project.

Trust) were most likely to get a judicial outcome (around 7% of disseminated cases). Of all cases, 11 (or 3%) resulted in a judicial outcome: 3 people were charged or summoned to appear in court, 2 were cautioned and 6 were the subject of community resolution. Of the remainder, 4 were transferred to another agency, 25 still had no outcome and almost 90% were not proceeded with on evidential and other grounds.

Assessment: what does the data say about the National Strategy's assumptions and recommendations?

The volume and costs of fraud

The overall 'cost' or losses associated with fraud remain unresolved, allowing the more exaggerated extrapolated claims to be used to justify the concerns over frauds. In practice, the National Strategy's figure of £3.1 billion of actual losses bears comparison to the 2021 Action Fraud figure of £2.35 billion although not significantly at variance at losses from other crimes (though there is a fuzzy line between staff and customer 'shrinkage', losses from customer theft in the retail sector are stated as £1.8 billion from over 16 million incidents: see British Retail Consortium 2024). The National Strategy is right to draw attention to the rise in the volume of frauds: however the figures are calculated, the rise in cases and losses year-on-year has been significant and sustained, though they have fallen subsequently towards pre-covid19 levels. On the other hand, the data would suggest most NFIB fraud categories may be voluminous but they are largely of low value. Thus, if financial cost to victims is a major indicator of 'seriousness' and in comparison to costs of other recorded crimes (and also in terms of competing agendas such as new national policing guidance on attending burglaries), it is understandable that police forces may wish to allocate staffing and other resources accordingly.

If the National Strategy had analysed the data and presented its arguments (as this article has sought to do), it might have had better evidenced grounds for responses that acknowledged that the vast majority of victims will not be engaged with the criminal justice process since, for a number of value, evidential and other reasons, their cases are unlikely to be disseminated to police forces. Further, of those cases that are disseminated, most will also not achieve an outcome likely to lead to the victim's cases being resolved to the satisfaction of the victims and perhaps of 'society'. This has implications for a range of responses, including additional resources for law enforcement (and the focus of those resources), as opposed to the centrality of prevention and the treatment of victims to both prevent frauds occurring in the first place and to minimise the high levels of repeat victimisation. Indeed, the focus on the 'how much' figures by those responding to TCSEW surveys—used by the National Strategy as its starting point as the 'by far most common crime' (HM Government 2023a: 3)—does not assist (and nor to a lesser extent, does the Action Fraud data) in answering some other important (and potentially difficult to answer)

questions as *part* of threat or supply side and demand-side assessments that should underpin a strategic approach.

Victims

Reducing victimisation or harm to victims

If the failure to draw on data that was available at that time as to why victims do not report to Action Fraud is one issue, then so is the National Strategy's failure to analyse what we might term 'active' victims and 'passive' victims, based around attitudes to risk. A better understanding is needed of this spectrum of people who are 'up for' new areas of potential profit versus those who are highly risk averse in terms of the likely impact of warnings from their information sources. FCA (2021) and other research at that time suggested that, for example, levels of correct understanding of plausibly legitimate rates of return on investment are low, indicating the need for better financial literacy among adults. However, in the contemporary world of truth decay, dire warnings from officials about crypto-currency value fluctuations and 'exit scams' may be disregarded as the efforts of 'The Establishment' denying opportunities for ordinary people. Likewise, those engaging in what they consider legitimate activities, such as lender loans or (mostly online) dating where any consequential financial transaction may be highlighted by financial institutions as risky, may be prepared to disregard warnings. Here the role of stakeholder intervention come into play.

As with many contemporary arenas of conspiratorial thinking, it is difficult to see who would count as an authoritative 'objective' source of information. Some would press for an appreciation of risk, risk appetite, and acceptable risk mitigation measures, including more proactive or intrusive measures that have been undertaken by banks in the past, to try to stop people being foolish with their money. Some of these processes are now built into banking apps, requiring customers to sign off that they are not being pressurised, etc., as are the efforts by banks to diagnose vulnerability individually or in categories, and calling the police in to assist in dissuading people from becoming victims of courier and allied frauds. While the National Strategy may identify the importance of addressing misuse of media tools or technology platforms—whether stopping cold-calling or blocking access fraudulent websites—as well as persuading financial, social media and other institutions to step up prevention measures, as the evidence has suggested, it is also essential to understand the dynamics of perpetrators (see Levi et al 2015 for publicly available analysis of patterns by NFIB fraud category where banks, for example, have tightened procedures and reduce levels of reported fraud).

This requires supply side analyses of the extent to which individuals those committing frauds are sector specialists or are versatile; 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; where the physical location of the execution of offences is or could be; and how far the changes in institutional cooperation and situational opportunity

prevention cause fraudsters or potential fraudsters to look elsewhere in terms of fraud types or modes of perpetration to commit fraud.

On both the demand and the supply side, there are also questions about how far victims are on the spectrum from passive to active (and how consistently) in relation to what areas, activities or technologies they engage with, what is their level or understanding of risk, and whether the focus should be 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. These all require detailed analysis of data on offenders' and on victims' behaviour and opportunities. These also require, for example, banks' own individual or collective analysis of customer fraud data as a fruitful avenue for future insights and prevention efforts, in order both to develop targeted and relevant awareness as well as prevention measures. One obvious consequence of not undertaking such assessments is a weak evidence base on which to predicate the balance between, for example, more law enforcement responses, or a significant shift to prevention and victim support, or whether the emphasis should be on requiring technology companies to improve the exclusion of fraud opportunities as opposed to educating the public in the risk associated with any online engagement. While all, or a permutation, of these choices are possible in principle, strategies are about evidence, priorities, and the resources that follow them—and thus why the failure to use available data means, as the 2006 Fraud Review noted, it would be impossible to develop a sensible national strategy for dealing with fraud.[24]

Further, in terms of developing iterations of such a strategy, such an understanding would have had the further benefit of thinking through how to develop more effective prevention approaches now and in the future. The nuances in the case study indicate, for example, that under-24s are disproportionately more likely to suffer from NFIB6B (Insurance Broker Fraud), where victims obtain insurance cover from a broker or someone purporting to be a broker but when a claim is made or the policy checked, they discover that they are not insured, or the cover that they have paid for and thought they had is not what they have) and NFIB1G (Rental Fraud), where paying advanced fees/rent for the rental of premises which, either don't exist, are not for rent, are already rented or are rented to a multiple of victims at the same time). Young people need to be to be encouraged to assess both probabilities and consequences, and this applies to investments including crypto-markets and (even at pre-teen ages) warnings about credulous following of social media 'influencers'. How we go about—and sustain—this process of education (and reinforcement of the lessons) remains a major challenge, given the uncertain impacts of nudges and warnings to date (Levi, forthcoming).

[24] It is noteworthy that an analysis of 'what works' in combatting fraud against organisations also suggests that high-quality evidence should be a priority to pursue in some areas, especially when the cost of fraud is very high or when the fraud problem is relatively less complex (see Button et al 2023a, b).

Supporting victims

Given that the majority of victims of fraud will not benefit from any law enforcement outcomes, the National Strategy did not explore the publicly available data on repeat victims which, by the Strategy's own estimation, is at least 18% and, according to the case study data, may average over 40%. Given the numbers of fraud victims that are theoretically eligible for care, it is obvious that proportionately few are likely—whatever the intentions—to receive such care in practice from the police or from other sectors. 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. Further, 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. While the Strategy mentions in passing social workers and charities, it spends no time working through where repeat victims might raise their concerns—doctors' surgeries (notwithstanding the strains upon them), Citizens Advice Bureaux, social care companies, and so on. Further, given the case study's analysis of the differential nature of risk and, for example, age or fraud category, where these and other organisations, such as the Integrated Health Boards, may help ensure that ongoing mental health and other services are available and accessible for at least some victims of fraud and certainly for those who are also victims of age or other potential vulnerabilities.

Apart from the question of the resourcing support for such large numbers, the National Strategy does not address the purpose of support (see Poppleton et al 2021). 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. Similarly, caring for victims 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. The National Strategy did not draw on Action Fraud data to understand the importance of a differentiated response, not only for repeat victims and which categories involve significant levels of repeat victimisation but also which sectors or which categories require what type of response?

Sanctions and reimbursement

The issue of sanctions is to be the subject of further work on 'penalties for fraud match the severity of the crime' and the use of 'civil debt recovery and other powers (to) recover more of victims' money' (HM Government 2023a: 24). The National Strategy remains relatively silent on mainstreaming the use of asset recovery and money laundering offences to secure funds for victim restitution. The data would have, 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), given the National Strategy guidance on other sources of restitution or compensation. These could include proceeds of crime recovered through conviction-based compensation orders, proceeds from international asset recovery,[25] or the proceeds of crime (including fraud) from Confiscation Orders, Forfeiture Orders and Civil Recovery Orders receipts, but which are likely to be a very modest proportion of total losses from fraud, and equally likely to be costly to administer (even after the few victims who would pursue civil remedies or have cases taken on by private prosecutions). Further, and while it should be recognised that the more innovative recommendations are about the supply side of frauds and the role of tech platforms, proposals for reimbursement of victims will continue to be a contested area, not in the least if the proposals do not include the tech platforms for their roles in facilitating frauds.

Certainly the liability of tech companies also needs to be aligned with what steps the National Strategy could have invoked to promote self-policing and prevention. Here, it should have explored or made explicit use of data on patterns and trends, including how fraud has changed in the preceding decade through the efforts of providers (see Levi et al 2015). Cases involving NFIB5A (Cheque, Plastic Card and Online Bank Accounts (not PSP)), and NFIB5B (Application Fraud (excluding Mortgages)) have dropped, largely through the efforts of financial services institutions. Similarly the Strategy did not seek to explore the current work of banks through banking apps, rapid scam responses under the 2020 Banking protocol and work to diagnose vulnerability individually or in categories, calling the police in to assist in dissuading people from becoming victims of courier and allied frauds. Within such changes, and according to the Financial Conduct Authority (FCA), 1.9 million UK adults with a day-to-day account had cards used without permission, money taken from their account without permission, lost money through unauthorised transactions, and/or experienced push payment fraud in the 12 months to February 2020, before the Covid-19 pandemic.[26] 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. The clear majority (88%) of those who recovered or tried to recover money say their provider treated them well (see FCA 2021). By the time this article is published, banks will be obliged to make full reimbursement to most victims, but other sectors of the economy are not similarly obliged, and this piecemeal approach will continue, though we envisage social media companies being obliged to do far more than at present.

[25] 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.

[26] 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.

Policing fraud

Law enforcement

There is no identifiable strategic approach or mechanism that geared resourcing and strategic direction on the basis of available data, particularly in understanding how to address and manage the expectations of the vast majority who have decided to report fraud but are entering a process where they are highly unlikely to receive any police intervention. The National Strategy did not draw the obvious inference from the volume-value contrast in the publicly-available and case study data: that most frauds fall clearly in the low value/high volume area, and that areas of life where most frauds occur are not the same as those where the greatest losses or harms occur (to both individuals and businesses). The fraud problems facing most of the population would *not* be those that (rightly or wrongly) would normally prompt police investigation, whether or not additional police resources are made available (i.e. where, given scarce resources, investigations will continue to be driven by being a linked series of cases and/or an organised crime group posing an ongoing threat and where the rationale lies in the use of cases as intelligence sent with but not part of the disseminations dataset). It is therefore, in prevention or awareness terms, important to explore what the data say about the types of fraud that are *not* selected for criminal investigation and whether there is room for a greater focus on victim support, awareness, and prevention to reduce the level of 'unsuccessful' reporting and harm and to mitigate any negative consequences stemming from raised expectations of victims knowing 'that the police will do something about their crime' when the data suggest otherwise.

Even in the area of what, within the totality of the public's exposure to fraud, is a minor role, the additional policing resource for investigations (from which also stems more prosecutions) appears to be neither for local forces nor for the vast majority of frauds which may fall below thresholds for detailed investigation. Half the promised additional officers were already in post at the time of the Strategy's launch, spread across the National Crime Agency (NCA), the City of London Police (CoLP, the national Lead Force for fraud) and the Regional Organised crime Units (ROCU). This would suggest that the Strategy may be continuing an identifiable shift in policing priorities and resources towards complex, sophisticated, and enduring patterns of criminal activity, which looked at 'the fraud problem' principally as a medium of exploitation by those already engaged in ongoing criminality and terrorism.[27] This thread runs through much of current UK government thinking about fraud and its attractiveness to OCGs (and their underlying management of risk in law enforcement [MoRiLE] methodology [Home Office 2018]) as a metric of harm and threat. Even if a 'reasonable' amount of extra resources were available to other

[27] 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.

police forces for fraud investigations, this alone would probably not reduce substantially the levels of such crime, unless the criminality was highly concentrated or amenable to investigation. The impact of extra police numbers on judicial outcomes remains to be seen. Police forces have recruited 'PROTECT' officers, but though this may be a good idea, their impact on the public and business victimisation is not yet known and may be difficult to measure.

Other strategies

The drivers for this shift in focus in terms of a law enforcement response are identifiable in a number of related strategies and plans, including the Economic Crime Plan (first issued in 2019 and reissued in 2023, addressing a joint public–private sector approach involving shared information, an enhanced law enforcement response and risk-based prevention), the National Cyber Strategy (first issued in 2016 and reissued in 2022), the Beating Crime Plan (2021), the Serious and Organised Crime Strategy (issued in 2013; reissued in 2018 and 2023), and the UK Anti-Corruption Strategy (first issued in 2017; reissued in 2023).

Of those which specifically address fraud, the Beating Crime Plan anticipates the Strategy's intentions in proposing a focus on online fraud and technology companies, replacing Action Fraud, increasing investigative capabilities and prosecutions, and better support for victims of fraud. The 2018 Serious and Organised Crime Strategy discusses the intended role of the Joint Fraud Taskforce (JFT[28]), prioritising 'designing out' fraud online, improving support to vulnerable and susceptible victims, and engaging with the information and communications technology industry; and the 2023 Economic Crime Plan. This latter Plan acts as 'the overarching document' for other strategies, widening its scope to encompass the work of the PSFA and central government departmental strategies, changes to criminal justice offences (including that of failing to prevent fraud) and processes, improvements to law enforcement capacity, information-sharing, and data protection, and developing 'an economic crime workforce strategy will look at skills, retention and partnerships across the economic crime workforce' including regulators and the private sector. The Economic Crime Strategic Board (ECSB) has strategic oversight of the Plan; The JFT reports to the ECSB.

The overarching document, focussing on economic crimes that 'fuel 'serious organised crime' and 'high harm financial crime', emphasises that the National Strategy also has, in terms of its law enforcement approach, a serious organised crime dimension. The new 'national fraud squad' is distributed across the NCA, CoLP and the ROCUs. Further, the National Strategy, consistent with the underlying trends towards locating fraud within an organised crime context, gives much emphasis to any additional police resource addressing fraud within such a context. Indeed, the 2023 national policing strategy issued by CoLP also has a key focus on

[28] In 2016, the Home Secretary set up the Joint Fraud Taskforce (JFT), a partnership between banks, law enforcement and government to deal with fraud and to focus on issues that have been considered too difficult for a single organisation to manage alone. It was closed in 2018 and revived in 2021.

Table 2 Themes Since 2006

	Awareness		Prevention		Enforcement		Evidence base	
	Issue	Response	Issue	Response	Issue	Response	Issue	Response
2006 Fraud Review	Many frauds could have been avoided if the victims exercised sensible scepticism or caution	Public awareness and information campaigns	A lack of awareness of organizations and businesses to their fraud exposure	Carry out a risk assessment of exposure to fraud and consider making appropriate investment to combat it; devising and circulating best practice and advice on systemic fraud prevention within industry and government	Fraud is not a national police priority. The case for major additional investment in fraud investigations will depend on measuring it better and reassessing its place amongst overall policing priorities	National lead force; regional fraud grouping; ring-fenced resources; making fraud a policing priority; extended range of non-custodial sentences; power to appoint a Receiver to recover property and distribute compensation. Awards; greater use of the administrative and civil court options	No estimates of the scale of fraud; no strategy	Fraud should be measured on a consistent basis across the economy; Government must formulate a national strategy

Table 2 (continued)

	Awareness		Prevention		Enforcement		Evidence base	
	Issue	Response	Issue	Response	Issue	Response	Issue	Response
2008 The National Fraud Strategy	High-quality advice is available on fraud through numerous channels, but it needs to be effective and targeted, encouraging people to behave in a way that denies criminals the opportunity to commit fraud	Efforts to raise public awareness must: build on past successes; target areas that need changing most; encourage people and organisations to take responsibility for protecting themselves	The most powerful way of tackling fraud is to eliminate the opportunities that allow it to happen in the first place	Individuals, businesses, and public organisations are able to prevent fraud; are able to do so, with access to appropriate advice from an authoritative source; take responsibility for doing so	Fraudsters will not stop committing fraud unless they face a credible threat of detection or sanction when prevention fails. Moreover, the general public will never trust a system that fails to address this challenge	Increasing the disruption and risk of detection and sanction that fraudsters face; regulatory and law enforcement agencies collaborating more effectively; ensure effective fraud investigation remains a mainstream part of policing; build the skills and capabilities needed to help police forces; deliver swifter justice for victims; support the victims of fraud; widen the range of fraud victims who are eligible for criminal compensation	Organisations must act together to disrupt fraudsters and their support networks. To do so effectively, they require a clear and shared framework that gives them a national overview of the most serious frauds	To do this, the harm from fraud will be assessed using criteria such as: volumes of crime and financial losses; impact on the victims; damage to public confidence; links to serious crime; systemic effects, such as disruption to markets

Table 2 (continued)

	Awareness		Prevention		Enforcement		Evidence base	
	Issue	Response	Issue	Response	Issue	Response	Issue	Response
2011 Fighting Fraud Together	Prevent more fraud by achieving a step change in awareness of fraud among the general public and organisations in the private, public, and third sectors and in their ability to protect and safeguard themselves.	Understanding behaviours and attitudes and, where necessary, changing them is vital for an effectively targeted strategic approach to reducing fraud	Prevent more fraud through stronger systems and controls in our businesses and public and voluntary services	Designing out fraud and making preventative checks before transacting with individuals and organisations	Tougher on fraudsters by disrupting and punishing them more efficiently and effectively	More effective civil and criminal processes, as well as greater early restraint of criminal assets; victims satisfaction rates increase as they are better supported by more efficient and robust justice, strengthened care arrangements and greater monetary returns from asset recovery and compensation	Fraud causes significant monetary losses to individual citizens, businesses and public bodies; criminals are now more organised; criminals are more technically capable; criminals increasingly operate across borders; fraud is linked to other serious crimes	Our strategic approach is firmly designed around our improved understanding of the fraud challenge; sets out the strategic mission we have set ourselves over the next four years based on our assessment of the fraud challenge

Table 2 (continued)

	Awareness		Prevention		Enforcement		Evidence base	
	Issue	Response	Issue	Response	Issue	Response	Issue	Response
2023 Fraud Strategy	It is unreasonable to expect the public to be on a constant state of high alert against fraud	Support more victims; reimburse more victims; better communication on awareness, protection and reporting	To stop people becoming victims and help them recover, we must empower them with the tools and knowledge to keep themselves safe and most importantly ensure they get their money back as quickly as possible	Stop criminals from abusing the telephone network; revolutionise tech company action to block fraud; help banks slow suspicious payments	Improve the criminal justice response and put more fraudsters behind bars	National fraud squad, more resources and training; Intelligence-led disruption; State-of-the-art reporting; Imprison more fraudsters and increase recovery of victims money through civil powers; Pursue fraudsters internationally	Fraud is the largest crime type and levels have grown in recent years	Not developed

intelligence-led policing against 'high harm' offenders (see City of London Police 2023: 14,20).

The 2023 National Strategy: fundamental shift or largely more of the same?

In summary, for all its merits and welcome extra focus on economic crime compared with earlier initiatives, the National Strategy did not visibly explore any lessons learned from past strategies, nor did it appear to substantively access, use, analyse, and interpret available data as a defensible evidence base to develop an approach that is strategic, prioritised, and innovative. What is presented is not so much a strategy as an Action Plan; many of the recommendations are neither new, nor specifically devised by or for the National Strategy. In many ways, this is a partial step back from the approaches proposed by the 2006 Fraud Review and the National Fraud Authority, but it is also apparent that the National Strategy has continued many of the themes and responses they first developed: see Table 2.

The Strategy is also aligned with many of the prevailing orthodoxies that have informed a number of other strategies and plans that have also referred to fraud. However, it is clear that the National Strategy takes its steer from its role within the overall Economic Crime Plan and its focus on serious and organised crime. It states it is 'accountable' to the ECSB while also stating that a 'programme board has been established to steer and govern delivery of the strategy, monitor progress, oversee the outcomes and manage key risks relating to reform. The board is chaired by the Home Office Director General for Homeland Security with representation from all delivery partners across government and law enforcement. The programme board is overseen by the JFT' (HM Government 2023a: 49).

The organisational changes since 2006 have reflected a clear directional shift in the law enforcement response to fraud which saw fraud both as an organised crime issue and a subset of the wider Economic Crime Plan. This was flagged up in the 2011 Fighting Fraud Together strategic plan, the grounds given for the abolition of the NFA, and the 2015 City of London Police (CoLP)'s Economic Crime Directorate's draft National Police Fraud strategy. While the 2011 national strategy review noted that 'the majority of frauds are not perpetrated by sophisticated, organised criminal gangs' (Fighting Fraud Together 2011: 10), both it and the 2015 National Police Fraud strategy implicitly assumed that, outside the very centralised and national approach to organised crime, 'local' fraud would be left to local force discretion where 'fraud is not prioritised strategically at the local level, neither in police and crime plans nor at an operational level by senior leadership teams' (Police Foundation 2018: 37; see also Gannon and Doig 2010).

The emphasis continues in the National Strategy which notes that 'the new Strategic Policing Requirement (SPR), which sets the capabilities the Home Secretary wants forces to have, gives greater prominence to fraud, which is captured within the serious and organised crime threat' (HM Government 2023a: 17) and with which a number of the proposed initiatives are viewed: thus, the NCA sees the National

Fraud Squad as a 'key initiative' that enhances 'the existing capabilities of organisations such as the NCA'.

While there may be more specific initiatives, the main themes reflect those of previous strategies and action plans. However, and unlike the specific resources and institutional ownership for the law enforcement aspects of the approach, the National Strategy was less than clear on the implementation and measurement of those areas relating to awareness, prevention, and victim support—who, for example, would be responsible for banning SIM farms or scam calls or taking down fraudulent websites, increasing access to and amounts for reimbursement, requiring tech companies to improve prevention and reporting as well as identifying and incentivising tech companies to combat frauds, identifying the appropriate agencies and funding them to ensure adequate victim support, and paying for communications campaigns? Some of the above are better demarcated than others in organisational responsibilities, and there is no obvious realignment or clarification in the National Strategy. This may be a task for the present government.

Finally, we note the relative absence of measurement or performance indicators in judging the progress or 'success' of the National Strategy beyond the single proposal in reducing the CSEW numbers by 10%. There is no timeline for delivery or implementation of the National Strategy 'key actions' ((HM Government 2023a: 5). This is in contrast to the intentions of the government's second Economic Crime Plan, whose progress measurement intends to collect and use improved data as well as developing:

> a Theory of Change which will inform the selection of indicators that are used in the outcomes framework for each action in the Plan. The Theory of Change will set out the inputs, outputs, outcomes (i.e. short-medium term results), and impacts (i.e. long-term results) of the actions within the Plan. It will enable us to better understand and assess effectiveness of the actions. Developing these indicators means tackling some long-standing data and evidence gaps in the field of economic crime. The work required will be extensive, challenging, and will take time—both to assess the feasibility of collecting new data and to develop suitable indicators, before beginning any new data collection (HM Government 2023b: 84–85).

Conclusion

In July 2024, ONS CSEW data[29] suggest that the dynamics of the overall fraud picture continue to reflect a range of issues raised in both the National Strategy and this article. There were over 3 million fraud incidents which represent a 10% decrease from the previous year and now 36 percent of overall crime. On the other hand, in terms of fraud offences recorded and collected by the National Fraud Intelligence Bureau (NFIB) from Action Fraud and two industry bodies, Cifas and UK

[29] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2024#fraud.

Finance, figures are up 7% on the previous year at over 1.2 million offences. Approximately 2.4 million fraud incidents recorded by the CSEW involved a loss (of money or property), and victims were fully reimbursed in 1.7 million of these incidents.

While the volume of fraud cases continues at high levels, the last—2022—CSEW data[30] to address the issue of value noted that, in the two thirds of incidents for which victims suffered a financial loss, over three quarters (77%) incurred a loss of less than £250, with the median loss being £79; around 14% incurred a loss of between £250 and £999 and the remaining 9% incurred a loss of £1,000 or more. More recent APP data[31] provided by banks show a similar distribution: only 4.6% of incidents relating to individuals involve amounts over £10,000; 70% lose less than £1000. The losses for this 4.6%, however, represent over 13% of the payment transactions and over 60% of total losses (PSR 2024).

Finally, 2024 Home Office data[32] noted that, of the fraud offences recorded by the police, a relatively small proportion were referred to territorial forces for investigation (2% for the year ending March 2024), although the number of fraud offences referred to forces for investigation increased by 37% (from 18,202 to 24,870). On the other hand, the total number of fraud offences assigned an investigative outcome decreased from 45,457 in the year to March 2023 to 39,354 (down 15%) in the year to March 2024. This is occurring in a context where HMICFRS (2024) continues to express concerns over the rise in fraud cases, variations in police responses and priorities, poor service to victims, and the need for a focus on prevention.

In terms of aspects of a policing response, we would note that enhanced policing of organised crime group engagement in frauds is a good thing and should have an impact on them and on the kinds of frauds they currently commit or might commit if left unmonitored and undisrupted. However, that impact assessment remains for the future. Overall we consider that such a patchy set of outcomes portrayed by the 2024 data confirms our concerns that the National Strategy is insufficiently grounded in careful analyses of existing data, crime patterns, and trends. Rather, it would appear to be influenced by the priorities of central government and what central government can do, as evinced by the focus and emphasis of other, related, strategies and plans. It is not surprising that the National Strategy does not offer 'a fundamental shift in our approach to tackling fraud' but rather offers largely more of the same (which, however, is better than 'the same'!). Given the attrition of cases from the CSEW data to those triaged for dissemination and acted against, some 98% of those experiencing or affected by fraud still will not enter the criminal justice process for investigative or prosecutorial responses. Thus, if the intention is to 'put protecting people at the heart of our response' (HM Government 2023a: 3) then, in strategic terms, there should have been a significant, even fundamental, shift towards

[30] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022.

[31] APP involves a criminal tricking their victim into sending money directly from their account to an account which the criminal controls, often by impersonating someone the victim has official dealings, such as an employer or solicitor.

[32] https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2023-to-2024/crime-outcomes-in-england-and-wales-2023-to-2024.

awareness, prevention and victim harm reduction on both the supply side and the demand-side of frauds.

This is *not* an argument against increasing police resources to increase fraud disruption and justice for victims; it is an argument for a broader attack on frauds which will have to be long term, because the general opportunities for frauds will not go away, whatever efforts are made to enhance policing services or to use public–private and private-private partnerships to reduce particular fraud risks and techniques in some areas. The approach would require interventions at national level, possibly requiring legislative reform (as has been battled over in the Online Safety Act 2023 and the Economic Crime and Corporate Transparency Act 2023) and sustained partnership working towards a more uniform response from payment and social media platforms, even when or if the pressure of prospective mandatory legislation eases. It would also require organisations other than the police to take up primary responsibility for increasing situational prevention measures for a range of frauds and for managing the victimisation risks and victim support dimensions of fraud. Such an approach will require a strong shift towards building up personal and third-party interventions and defences against frauds on a coordinated and resourced basis for, for example, encouraging people to use the internet safely and avoid dangerous activities, subject to their risk appetites and the consequences of their risky behaviour for others.

This will plausibly focus more on protecting the victims than on discouraging potential offenders via policing, and on seeking to build up a sense of security and resilience. Here—notwithstanding well-known campaigns around seatbelts and smoking (or even use of mobiles in cinemas)—the challenge would be not just to warn people through media campaigns about the dangers—as has been happening—but to focus on sustained help for potential victims to become 'fraud conscious' or 'fraud alert' in carrying out any transaction, particularly online. The intention is to provide an evidenced platform from which to improve the general 'fraud' health or welfare of the population, and not just to help the far lesser number of fraud victims whose cases are reported to, or enter, the criminal justice process (and whose satisfaction levels have not been measured properly if at all systematically).[33]

The shift away from the police, with others taking primary responsibility for encouraging people to use the internet safely, reducing if not preventing levels of future frauds, and seeking to build up a sense of self-aware security and resilience, requires the organisation and coordination of both new and existing initiatives, and the engagement of a wider network of relevant organisations. The Police Foundation already proposed during the gestation of the National Strategy a separate crime prevention agency to address crime and harm prevention. This would not be a policing institution but which would look to ensuring that 'all sectors of society should play their part in crime prevention and that crime control should not be seen as a "police problem"' (Police Foundation 2022: 62). Given how many frauds there are, and the

[33] The article does not discredit victim and witness care programmes, both of which are important as shifts towards a victim-focussed rather than state-focussed justice system, though we await public evaluations of their impacts. But except when combined with learning how to avoid fraud – which may be facilitated by AI—this 'support' is different from a fraud prevention focus.

current mechanisms for awareness and prevention, existing measures may need a structured, coordinated and continuing outreach programme by trusted (and trust*worthy*) organisations and persons. Such measures would also be central to managing the numbers of victims contacting the more intelligently designed and better resourced successor to Action Fraud. It will have to manage their expectations about the practical effects of knowing 'that the police will do something about their crime'. It will also aim to reduce repeat victimisation and to reduce the longer term impact of fraud on them.

Analysis of the data would place prevention-based interventions that have less to do with tackling offenders than an evidence-informed approach that will engage with community organisations, with health professionals, and with the police. This will encompass both deterrence and *public reassurance* that some of their concerns are being paid attention to. The Strategy offers some progressive measures that begin to shift the dial via pressures on more parts of the private sector and modest changes in the public sector. The value of sectoral charters remains to be seen, but our interviews reveal widespread scepticism (fair or unfair) about the total impact of these well-intentioned measures on frauds, possibly reflecting more general distrust of business and government. Given the scale and demographics of individual and repeat victimisation and the current mechanisms for awareness and prevention, ongoing measures need to be developed that address frauds holistically, via interventions with both offenders and (primarily) with victims. Only with such central and local measures at scale is the National Strategy likely to mark a fundamental shift in the approach to tackling fraud**.**

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

British Retail Consortium. 2024. *Crime survey: 2024 Report*. London: British Retail Consortium.

Button, M., B. Hock, D. Shepherd, and P.M. Gilmour. 2023a. Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2023.100012.

Button, M., B. Hock, D. Shepherd, and P.M. Gilmour. 2023b. What really works in preventing fraud against organisations and do decision-makers really need to know? *Security Journal*. https://doi.org/10.1057/s41284-023-00402-4.

City of London Police. 2023. *National policing strategy for fraud, economic and cyber crime 2023–2028*. London: City of London Police.
Committee of Public Accounts. 2022. *The Department for Work and Pensions' Accounts 2021–22 – Fraud and error in the benefits system.* HC 44. London: House of Commons.
Committee of Public Accounts. 2023. *Progress combatting fraud*. HC 40. London: House of Commons.
Committee of Public Accounts. 2023. *Tackling Fraud and Corruption against Government*. HC 1230. London: House of Commons.
Doig, A., M. Levi, and S. Johnson. 2001. Old populism or new public management? Policing fraud in the UK. *Public Policy and Administration.* 16 (1): 91–113.
Financial Conduct Authority. 2021. *Financial lives 2020 survey: The impact of coronavirus*. London: Financial Conduct Authority.
Fraud Review. 2006. *Final Report*. London: Attorney-General's Office.
Gannon, R., and A. Doig. 2010. Ducking the answer: Fraud strategies and police resources. *Policing and Society* 20 (1): 39–60.
Heeks, M., Reed, S., Tafsiri, M. and Prince, S. 2018. *The Economic and Social Costs of Crime*. Second Edition. Research Report 99. London: Home Office.
HM Government. 2023. *Fraud Strategy: Stopping Scams and Protecting the Public*. CP839. London: Home Office.
HM Government. 2023b. *Economic Crime Plan 2*. London: Home Office.
HMICFRS. 2019. *Fraud: Time to Choose. An inspection of the police response to fraud*. London: HMICFRS.
HMICFRS. 2021. *Spotlight report. A review of Fraud: Time to choose. A revisit of the 2018 fraud inspection to assess progress of the recommendations and areas for improvement*. London: HMICFRS.
HMICFRS. 2024. *State of policing: The annual assessment of policing in England and Wales 2023*. London: HMICFRS.
House of Commons Justice Committee 2022. Fraud and the Justice System. HC12. London: House of Commons.
House of Commons Library. 2022. *Police service strength*. London: House of Commons.
House of Lords Fraud Act 2006 and Digital Fraud Committee. 2022. *Fighting Fraud: Breaking the Chain.* HL Paper 87. London: House of Lords.
Office, Home. 2018. *Management of risk in law enforcement (MoRiLE) Based scoring: standards*. London: Home Office.
Levi, M. (forthcoming). 'Human, political and technological factors involved in a public health approach to fraud'. Paper first presented at Human Factors in Cybercrime Conference, Halle, Germany, 2023.
Levi, M., and A. Pithouse. 1992. Victims of fraud. In *Unravelling criminal justice*, ed. D. Downes. London: Macmillan.
Levi, M., and M. Maguire. 2012. 2012. 'Something old, something new; something not entirely blue: Uneven and shifting modes of crime control.' In *Policing: Politics, culture and control: Essays in honour of Robert Reiner*, ed. T. Newburn and J. Peay, 195–218. Oxford: Hart Publishing.
Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. 2015. *The Implications of Economic Cybercrime for Policing*. City of London Corporation. http:// orca- mwe.cf.ac.uk/ 88156/ 1/ Economic-Cybercrime- FullReport.pdf.
Levi, M., and A. Doig. 2019. Exploring the "Shadows" in the implementation processes for national anti-fraud strategies at the local level: Aims, ownership, and impact. *European Journal on Criminal Policy and Research* 26: 313–333.
McNabb, D.E. 2015. *Case research in public management*. Abingdon: Routledge.
National Audit Office. 2022. *Progress combatting fraud*. HC 654.London: NAO.
NERA. 2000. *The economic cost of fraud*. London: NERA Associates.
NFA. 2011. *Fighting fraud together*. London: Home Office.
Office for National Statistics. 2022. *Nature of crime: Fraud and computer misuse year ending March 2022*. London: ONS.
Office for National Statistics. 2019. *Appendix tables: Nature of fraud and computer misuse in England and Wales, year ending March 2019. Table 13.* London: ONS.
Osifo, O.C. 2015. Public management research and a three qualitative research strategy. *Review of Public Administration and Management.* 3 (1): 1–8.
PSR. 2024. *APP scams performance report.* https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/.

Police Foundation, 2018. *More than just a number: Improving the police response to victims of fraud*. London: Police Foundation.

Police Foundation. 2022. *A New Mode of Protection: Redesigning Policing and Public Safety for the 21st Century. The Final Report of the Strategic Review of Policing in England and Wales*. London: Police Foundation.

Poppleton, S., K. Lymperopoulou, and J. Molina. 2021. *Who suffers fraud? Understanding the fraud victim landscape*. London: Victims Commissioner.

Royal United Services Institute. 2022. *Towards a new model for economic crime policing target 2030*. London: Royal United Services Institute.

Saunders, M., P. Lewis, and A. Thornhill. 2009. *Research methods for business students*, 5th ed. Harlow: Pearson Education Limited.

Skidmore, M., J. Goldstraw-White, and M. Gill. 2022. 2022. 'Understanding the police response to fraud: the challenges in configuring a response to a low-priority crime on the rise.' In *Frauds and financial crimes: Trends strategic responses and implementation issues in England and Wales*, ed. A. Doig and M. Levi, 28–38. New York: Routledge.

Skidmore, M., and B. Aitkenhead. 2023. *Understanding the characteristics of serious fraud offending*. London: The Police Foundation.

Social Market Foundation. 2022. *Fraud is now Britain's dominant crime, but policing has failed to keep up*. London: SMF (https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/).

Social Market Foundation. 2023. *Fraudemic: Adding to the evidence base on the scale and impact of fraud on the UK*. London: Social Market Foundation.

Spotlight on Corruption. 2022. *Closing the UK's economic crime enforcement gap: Proposals for boosting resources for UK law enforcement to fight economic crime*. London: Spotlight on Corruption.

Supreme Court. 2023. *JUDGMENT Philipp (Respondent) v Barclays Bank UK PLC (Appellant)*. London: Supreme Court.

Treasury Committee. 2022. *Economic Crime*. HC 145. London: House of Commons.

Yin, R.K. 2009. *Case Study Research: Design and Methods. 4th Edition. London: Sage. See also Yin, R.K. 2003. Applications of Case Study Research*, 2nd ed. London: Sage.

Zhang, Y. and Wildemuth, B.M. 2017. Unstructured Interviews in Wildemuth, B. M. (ed). *Applications of Social Research Methods to Questions in Information and Library Science* (2nd Edition). Santa Barbara, California, and Denver, Colorado. Libraries Unlimited.