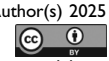
Special Issue: The Human Factor in Cybercrime

European Journal of Criminology

Human, institutional, political and technological factors involved in a public health approach to frauds against individuals

European Journal of Criminology
1–25



DOI: 10.1177/14773708251341076
journals.sagepub.com/home/euc


Michael Levi
Cardiff University, UK

Abstract

The paper describes briefly evolving data on frauds against individuals globally, political reactions to those frauds and how they vary. Based on an earlier study for West Midlands Police and Crime Commissioner's Office, it reviews the dynamics of developing approaches to the policing of cyber-enabled frauds against 'the public' – focused particularly on the UK and how this might differ in other European countries; what is known about public and private sector measures taken to reduce actual frauds and their impacts; and what a public health approach to frauds to parallel approaches to violence reduction might entail. Interventions might include: shrink the pool of potential and actual offenders; reduce the number of victims; reduce the number of *repeat* and 'especially vulnerable' victims; reduce the *size* of frauds within each fraud category; repair the well-being of distressed victims and reduce the 'unproductive' fears of the general public (consistent with giving them the motivation and tools to resist offers that may later become frauds). Greater attention is now being paid by many governments, financial institutions and law enforcement to frauds on the public, but knowledge is negative or weak about many impacts of law enforcement and public health interventions, including counter-fraud advertising for the general public. Although some initiatives are promising, warning the public will have only a moderate impact unless it takes account of the dynamics of fraud techniques, social engineering of victims and the need for support for 'the vulnerable', a term that requires greater clarity. More needs to be done both to create space for earlier and post-fraud education, mental health support and impact measurement. At present, a public health approach to fraud lacks some financial and institutional underpinnings to take off, but it is a conceptually appropriate approach that requires more clarity, political and resource support for enhanced effectiveness.

Corresponding author:
Michael Levi, School of Social Sciences, Cardiff University, Glamorgan Building, King Edward VII Avenue, Cardiff CF10 3WT, Wales, UK.
Email: levi@cardiff.ac.uk

Keywords
Crime prevention, cyber, fraud, policing, public health, white-collar crime

Introduction

This article describes and seeks to account for both police and non-police efforts to combat and reduce cyber-enabled frauds, a large and growing sub-set of frauds.[1] This analysis is placed within moves towards a public health approach to cyber fraud in the UK and potentially elsewhere in Europe, whose plausible impacts are critically examined.

In England and Wales, fraud now accounts for half of crimes by volume (ONS, 2025a; OSR, 2025) and almost certainly far more by financial cost. As measured by national/EU crime surveys, by police-recorded crimes and by payment card industry reports, frauds against individuals have been rising and have become a larger proportion of total crime in many countries over the past decade. Frauds have also become 'democratised', affecting a very broad range of individuals by age, ethnicity and socio-economic status, at least throughout the Global North and BRICS (for summaries, see Aebi et al., 2025; Button et al., 2023; Levi, 2023). However, not all sub-types of fraud change in the same direction or rate (e.g., Doig et al., 2025; UK Finance, 2024).

What is being done about all this online fraud? Collaborative public–private partnership working is a mantra of international counter-fraud and (separately) anti-money laundering policy. Given poor police capacities and capabilities, delays in reporting and the internationalisation of offender locations and money laundering, it has also become an international mantra among law enforcement and officials that society cannot prosecute its way out of fraud (author interviews, 2006–2025). This article will consider the difference between public–private collaboration and a broad public health approach to online *fraud* reduction.

Why examine public health approaches? Multi-agency public health approaches have been relatively successful in reducing violent crime in Scotland (Arnot and Mackie, 2019), and in modified form, have been adopted in parts of England and Wales and internationally, particularly against knife crime, alcohol-related and other violence (Shepherd, 2007, 2023). As the College of Policing and Public Health England (2019)[2] have pointed out:

> Public health approaches involve interventions delivered at population level and targeting resources effectively through increased understanding of the population….

The components of the approach therefore include:

- Using the population/large group as the unit of analysis and intervention;
- Looking behind 'presenting problems' to understand what is driving them;
- Starting from the principle that prevention is better than cure (or better than post-event harm mitigation);
- Skilled use and interpretation of data towards the evidence base necessary to ensure that interventions are designed, delivered and tailored to be as effective as possible;

- Developing coordinated interventions at primary, secondary and tertiary levels – primary intervention to promote awareness of risk, generally or in relation to specific risks; secondary specific or structured interventions to mitigate or disrupt an at-risk activity; and tertiary interventions to prevent or mitigate harm and loss among repeat victims.

It does not currently treat crime and risk through an epidemiological framework as something that spreads through the population.

Background to and methods of the study

After a scoping exercise, and given the ratio of reported frauds to policing resources, a team led by the Author was engaged by the West Midlands Police and Crime Commissioner in 2021 to examine the data (a) from reports from the West Midlands individual and organisational victims to the National Action Fraud reporting centre and (b) forwarded by the National Fraud Intelligence Bureau (NFIB) to the West Midlands police (WMP) on the basis of investigative potential (irrespective of the WMP *capacity* to do so). We were then to consider if there was a basis for a public health approach to fraud, and what forms that might take. This was a very low-budget study to obtain and analyse regional data and experiences and to suggest future practice changes, rather than a hypothesis-driven/experimental project. No major differences exist in the patterns of data at a West Midlands compared with England and Wales level, so given the elapsed time, more recent ONS national data have largely been used in this article.

One dataset was related to over 20,000 reports of fraud from May 2020 to June 2021; another comprised NFIB disseminations of over 1000 reports for investigation by the WMP between April 2020 and March 2021, of which fewer than 10% (1% of the reported frauds) resulted in a judicial outcome by the end of 2022. No further action was taken in over three quarters of the reports, largely because of evidential challenges and resource shortages. Raw data are highly classified, but demographic findings have been published (Levi et al., 2023) and inform the practice and policy discussions that follow. The data analysis was supplemented by author interviews with police, trading standards and private/third sector representatives at the time, and the author's interviews and collaborations with British, European, Europol and Interpol law enforcement about allied themes over the past decades are used to illuminate the review, alongside research on frauds and responses during COVID-19 (Levi, 2022).

The research goal here is to outline measures that have been employed against a range of 'ordinary' frauds, and the plausible potential for better impacts, including whether in this context, 'a public health approach' is more than a badge, though badges *can* motivate action. It will consider the *politics* of implementation, an aspect often neglected in classic situational crime prevention and routine activity studies. These measures will be examined within a broader European and Global context, since offender location has no natural limits in cyber frauds.

Consumer frauds and political/policing pressures to deal with them

'Fraud' and 'cybercrime' are a growing part of public and political consciousness in the UK and many parts of the Global North, largely because of rising prevalence and media coverage of fraud/scam victim stories of a more visceral kind than observed in 'white-collar crime' and 'cybercrime' coverage earlier this century (Levi, 2006, 2008). Fear of cybercrime is high generally in Europe (Cook et al., 2023); and in Germany (Birkel et al., 2020) and Sweden (Brå, 2024), both men and women expressed far more concern about becoming victims of fraud on the Internet than about any other type of crime. Like other crimes, fraud data reflect what is done to combat them, though data are not refined enough to account for why fraud rates differ within or outside Europe. The fraud rate per European country representatively sampled is (in descending frequency) France, Spain, UK, Portugal, Germany and Italy; and for repeat fraud victimisation, it is Germany, Spain, France, UK, Portugal and Italy (Hyde and Gibson, 2024).[3] Actual fraud impacts (on people, business and government) include affordability and resilience rather than just financial losses (Dupont, 2019; Levi et al., 2023): financial recovery may not eliminate the psychological impact of being defrauded or fear of future frauds. UK Finance (2024) and EBA (2024) note high total costs of mostly cyber-enabled payment card frauds. Yet, median fraud costs for individuals reporting fraud in the West Midlands were under £80 (Levi et al., 2023) and are just over £100 for England and Wales (ONS, 2025b, Table 9a). Earlier police data showed the median losses across all fraud types – 2013–2014 – ranged from £112 for misuse of phone contracts to £38,974 from pension fraud. Those categories with the biggest losses to individuals – such as pensions and financial investment frauds – were least related to cyber-enablement or cyber-dependency (Levi et al., 2017). Global online surveys (GASA, 2024) and police data show large rises in fraud in Asian economic hubs like China, Hong Kong, Singapore, South Korea and Taiwan, and their police show high levels of proactive counter-fraud activity and public warnings, though there are no published data on public confidence about responses to fraud.

However, changes and levels of crime rates and costs alone do not drive changes in policing: shifts in police orientation and resources normally require moral and institutional entrepreneurship, including pressure from formal accountability and/or from pressure groups, plus media campaigns (Bowling et al., 2019). Fraud and cybercrime policing are so marginal that they are not mentioned in the history of post-1945 policing in Britain by Newburn (2024). The 2-year UK National Fraud Strategy (Home Office, 2023) and subsequent National Policing Strategy (CoLP, 2023) stress the threat of 'fraud' to national security, and its links with Organised Crime Groups, as well as the need to better protect and serve victims. ONS (2025a) data show there is one fraud incident for every 13 adults in England and Wales annually. Yet, when British politicians (and likely those in other parts of Europe) talk about the need to fight 'neighbourhood crime',[4] they seldom mention any types of fraud.[5] This is despite the fact that though *online offenders* may be far distant, many online consumer scams and offline doorstep deceptions and affinity frauds occur in our neighbourhoods or even in our homes, so they may properly be called 'neighbourhood crimes'.

Political reactions to fraud vary within Europe, for reasons that are not yet clear, and this has implications for resources. Combating fraud and cybercrime are part of the core functions of Europol, Interpol, the European Public Prosecutor's Office and Eurojust, for analysis, collective action and enforcement, and these are an important part of their institutional legitimation with stakeholders. Serious UK-led attempts at international leverage and collaboration have begun,[6] though there is no intergovernmental mechanism with a mandate for online and/or offline fraud reduction as there has been for decades for bribery and corruption, drugs and money laundering. International not-for-profit and trade bodies act as pressure groups for governments and enforcement bodies to do more against frauds.

Policing and criminal justice responses

What has been the response of law enforcement to these growing 'economic crime' rates? Fraudsters and victims can be elite, quotidian or 'organised crime', and what kind(s) of frauds and fraudsters are being targeted is seldom explicit. UK local policing has little capacity for any complex or time-consuming cases, and specialist units (including the UK Serious Fraud Office) must ration their limited capacity. UK individuals and businesses alike can expect typically poor criminal justice responses if they report fraud (Button, 2021; CoLP, 2023; HMICFRS, 2024; Levi et al., 2023); and those counter-fraud professionals and police interviewed in the West Midlands were conscious of these negative likely outcomes. There is little systematic material on fraud policing in Europe, and author interviews (2023–2024) suggest that – except Italy in dealing with economic crimes committed by mafia-type organisations[7] – European law enforcement/prosecution bodies have not raised their capacity and capabilities to match the changing frauds. Poor *percentage* outcomes can occur even in countries where there is little formal discretion *not* to prosecute once there is sufficient evidence, and some German courts are clogged up with tax fraud and money laundering cases already (Author interviews, 2024–2025).[8]

The limitations of current criminal justice are clear. One in seven CSEW-measured frauds/attempts are reported to the police. Until the end of March 2023 (ONS, 2023a: Table 4.2), 2% of police-recorded frauds were sent to UK territorial police forces for investigation, but only 3904 frauds (0.35% of police-recorded frauds and 0.05% of CSEW-reported frauds) ended in criminal charges, an even lower proportion than in the West Midlands. The larger the frauds, the longer the elapsed time to reporting and prosecution, and the greater the difficulties in scheduling trials. Fraud and cybercrime policing will receive close attention in future inspections (HMICFRS, 2024), perhaps also because of worries that inaction on frauds may bleed legitimacy from the police.

Notwithstanding government funded increases in 2023–2024 to central and regional policing of 'organised fraud', it is highly unlikely that the current 1–2% of UK police resources devoted to fraud will increase dramatically in competition with claims for more policing of violence against women, knife crimes, organised immigration crimes or 'public disorder'. Even if far more arrests were made, UK austerity cuts in the court system can mean year-long trial delays for not guilty pleas to fraud charges.

Given fraud rates and the fact that most high harm and high frequency volume fraud suspects are outside easy jurisdictional reach,[9] principle and pragmatism suggest a less police-centred approach to fraud control.[10] When collected, the fraud and criminal justice figures (and their rate of change) will vary internationally, but even in countries such as South Korea that have long devoted far more resources to fraud policing (Loveday and Jung, 2021; Na, 2023), many challenges remain.

Multi-agency, public–private and public health approaches to frauds aimed at private individuals

Some seek 'justice' as an end in itself as a response to crime: they will largely be disappointed by responses to *any* type of fraud. By contrast, a public health approach – though not uniquely – reflects a utilitarian evidence-based effort to reduce harms. There is very limited evidence of 'what works' to reduce cyber-enabled/assisted frauds against the public (see e.g., Button et al., 2024; Cross, 2016, 2020; Prenzler, 2020). *A priori*, there are several ways in which we might reduce these harms, for only some of which there is space here to discuss:

- shrink the pool of potential and actual offenders;
- reduce the number of victims;
- reduce the number of *repeat* and 'especially vulnerable' victims;
- reduce the *size* of frauds within each fraud category and overall;
- repair the well-being of distressed victims and;
- reduce the 'unproductive' fears of the general public (consistent with giving them the motivation and tools to resist offers that may later become frauds).

It is not self-evident that *enforcement* agencies are or should be willing to perform many of these tasks, but if not them, who *would* carry them out? Levi and Maguire (2004) noted that at the beginning of this century, very few EU countries conceptualised policing of organised crime as engaged in 'the preventative turn': operational enforcement was the normal mode, except for the UK, Netherlands and Sweden. It is moot how far this picture has changed. The evolution of public–private partnerships in fraud and in e-crimes may be found elsewhere (see e.g., Dudink et al., 2023; Ilbiz and Kaunert, 2023; Levi, 2010; Meerts et al., 2025; Southworth, 2013), but such cooperation long preceded the development this century of internet commerce and of 'cybercrime' as a police issue (Levi, 2008, Levi et al., 1991). From 2002 onwards, UK payment card and later motor insurance sectors opted to pay for industry-wide intelligence units and for specialised police fraud units to assure some (and more consistent) police response to victimisation[11]: though the police still choose their own investigations, this pragmatism about State functions would be regarded as inappropriate in many European nations, for example, Germany and Italy. Since such investments have to be justified, the preventative impact of these units is measured roughly by multipliers of what the Organised Crime Groups arrested might have been expected to cost the industry if they carried on offending. In addition to the police, UK National and Local Trading Standards officers have

consumer fraud enforcement and prevention functions but have to ask the police for help if they wish to make arrests (Levi et al., 2023; Phillips, 2017).

Modifying underlying risk factors to reduce the likelihood that a person/firm will become either a victim or a perpetrator of a crime can operate on any or all of: victims, 'vulnerable people' (i.e., people who are at risk of multiple victimisation and/or who would be specially harmed if victimised), offenders (at home and overseas where reachable), commercial transactors, and third party 'capable guardians'[12] in the public, private or third (i.e., not for profit) sectors.[13] European offender outreach and general cybercrime prevention will not be discussed here (see Brewer et al., 2019; Collier et al., 2019, 2022, 2023; Moneva and Leukfeldt, 2023; van der Wagen et al., 2021), but are more developed for younger cybercriminals than for fraud. It is difficult to evoke conscience or to enhance actual and perceived criminal justice risks among Global South online fraudsters (Cretu-Adatte et al., 2024; Whitty, 2018), *a fortiori* when there is local corruption or state sponsorship/toleration of 'economic warfare', though there are ongoing EU, UK and US police efforts to enhance arrests and mutual legal assistance from West African police and prosecutors. Understanding and reshaping drivers of fraud in the general population is a component of public health approaches, but situational and 'organised crime' drivers for volume fraud have received the most attention. We will focus here on efforts for and with victims, repeat victims, and the general public. Some measures discussed aim to have impacts on all three. There is no space to discuss all the items mentioned in Table 1, but they are there to stimulate further thinking and action.

Incentivise potentially capable guardians

Capable guardianship makes most sense in the context of resources deployed against the problems it confronts, for example, the number of potential and actual offenders and victims of particular sorts of fraud. Sidebottom and Tilley (2023) criticise (non-fraud) public health approaches for their neglect of situational approaches in favour of general population-based early intervention programmes, but there are many situational and collective private initiatives against fraud, even if much impact measurement is underdeveloped and/or unpublished. In routine activities theory and situational crime prevention terms, this means making third party guardians and 'suitable targets' more capable of resisting what Sparrow (2008) termed 'conscious opponents'.

Some forms of public–private and inter-private cooperation happen relatively consensually and organically. After a report on prevention of cheque and credit card fraud (Levi et al., 1991), assisted by significant Ministerial pressure to respond to it and data protection legislation that permitted information-sharing for the purpose of crime prevention, bankers and police began to collaborate systematically, with significant fraud reduction impacts (Levi and Handley, 1998), though long-term funding from banks was required to enable more active policing. Less organic changes can be applied by Regulators, within their legal mandates, for example, tough new fraud reimbursement rules for banks from 7 October 2024, notwithstanding Conservative government pressures to mitigate and delay this.[14] The UK Payment Services Regulator defied pressures not to publish banks' differential reimbursement rates (PSR, 2024), shaming them and making rules to

Table 1. Primary, secondary and tertiary interventions against frauds.

Primary interventions
Advertising campaigns by public and private actors; fraud advisory websites; direct customer communications from banks and fintechs; Money Which? Subscriber information on scam alerts; News media stories; 'Prevent' outreach to cyber-offenders; thematic inserts into tv and radio dramas, podcasts and TikTok; tighter controls over company formation and professional fraud enablers, with market testing to examine how they operate and work.
Secondary interventions to mitigate or disrupt an at-risk activity
Account freezing of suspects; commercial monitoring of card and other transactions using historic spending algorithms; counter money mule activity to disrupt and/or arrest; data sharing private–private and private–public; Europol, Interpol and National agency cross border intelligence collation and investigations; informants/covert human intelligence sources; Financial and professional sector suspicious activity report follow-up; open and dark website takeovers and takedowns; proactive/reactive police operations including arrests and other disruptions; social media self and other monitoring for adverts claiming untrue authorisation of firms and deep fake ID.
Tertiary interventions to prevent or mitigate harm and loss among repeat victims
Banking protocol for bankers to call the police and delay transfers; civil litigation; civil and criminal asset freezing orders; police and non-police victim care; suspension of faster payments; lawful phone interception services to protect 'vulnerable persons'.

improve their conduct. The EBA (2024) asserts that strong customer authentication mandated under the EU Payment Services Directive (PSD2) helped to reduce fraud.

There is explicit movement to 'responsibilise' social media firms, who are accused by UK banks and the public of not paying their fair share of the crime opportunity externalities generated by their commercial products (see also Ofcom, 2023, 2024).[15] Political compromise led to communications technology and social media industry agreements with the Home Office to do more against fraud, but notwithstanding the Online Safety Act 2023, anti-fraud regulatory powers will come into play long after child safety powers.[16] See the Australian Scams Prevention Framework Bill 2025 and Singapore Protection from Scams Bill 2025 for active efforts elsewhere, though Singapore's Shared Responsibillity Framework reimbursement provisions are less extensive than in Australia or the UK.

Some social media (and financial services) businesses are reluctant to share data universally because 'free riders' can piggy-back upon their costly investment in fraud prevention technologies (Author interviews, 1990, 1999, 2023). There remain serious challenges in many countries of persuading or requiring commercial businesses to sacrifice substantial profits for the common good. Large information flows occur from victims to the private sector and vice versa, and between trusted third parties, in many cases unmediated by police but subject to variable national data protection laws.[17]

Close down opportunities for fraudsters

One source of mass leakage for identity 'thefts'[18] is weak data storage. In addition to quicker patching and multi-factor authentication, individuals are encouraged to make

suspect email reports (SERs) to the National Cyber Security Centre, which takes action to remove URLs when there is sufficient actionable intelligence.[19] This SERs database will be merged with the fraud one when Action Fraud is relaunched in 2025, after a £150 m government investment for more staff and better technology.[20]

In February 2025, under growing international public and media pressure, the Thai authorities cut off electricity to Chinese-run scam factories on the Myanmar border which 'employed' many trafficked workers.[21] This indicates the political elements in implementing this situational crime prevention measure which could have been done much earlier; there may be other opportunities for analogous interventions – displacement effects can be studied, and it may take criminal networks time to find corrupt protection. By May 2025, some scam centres allegedly had by-passed the Thai electricity controls by using portable Internet packs and connecting to services such as Starlink, though this might not work as well at scale, and they presumably could be de-registered if there was the motivation to do so.

Cut down the size of frauds

For frauds like embezzlement, payment card and romance frauds that typically occur over time rather than as one-shot events, we need to think beyond the binary fraud/no fraud. Even prior to the growth of e-commerce, card schemes intervened to identify 'points of compromise' in merchant systems and – aided by individual histories' spending algorithms – to warn customers and freeze suspected compromised merchant and consumer accounts to reduce their own and the public's losses. It is commonplace for cardholders to get proactive communications from banks asking if transactions are theirs, long before they would have realised they had been defrauded.

A different dimension of cutting down fraud size is identifying and informing people that they are victims. In romance and cryptocurrency/Ponzi investment scams, bleeding people dry is part of a *process*, and banker and police interventions to stop this happening are sometimes met by resistance from those in denial about the risks from people in whom they believe, though the frequency of denial is undocumented. It is moot whether fraud reimbursement requirements encourage such resistance. Many UK banks ban crypto investments, so customers would have to lie to them about the purpose of their expenditures to get the banks to process payments. Romance fraud victims may have been socially engineered to reject such 'help', and many UK banks feel obliged to let the transfers through, even if the customers were internally listed as 'vulnerable'. In some jurisdictions – including the UK and the Netherlands – the rise in frauds has led countries to allow slower payments under some circumstances to enable more frauds to be prevented or reduced in scale.[22] Australian banks can in 2025 prohibit funds transfers where customers are deemed to be 'vulnerable' (ABA, 2024; author interviews, 2025); by contrast, Swiss bankers would find it inconceivable to prohibit a lawful transfer that a customer wished to make (Author interviews, 2024).

Reduce the number of victims

Although not logically incompatible, there can be a cultural tension between responsibilising individuals by giving them the tools to make more rational decisions, on the one

hand, and more paternalistic social approaches to build up kinship/neighbourhood defences against frauds, on the other. Primary interventions include general financial education in early years – from 2025 being introduced patchily in England – and/or when closer to making investments (to combat poor judgements about investment/savings risks), general educational awareness of fraud and cyber security (for scam and phishing resistance), specific counter-fraud advertising and procedures in online banking apps that aim to force cognitive breaks in decisions that otherwise could end in Authorised Push Payment frauds. This is done by requiring customers to sign off that they are not transferring funds under pressure, and they are not purchasing crypto and other items deemed risky. Many UK, Danish and Dutch banks send messages to customers about fraud techniques and things they should avoid doing though 'in the moment'; such advice is sometimes overridden by social engineering (see Jensen et al., 2024).

Early years of education in calculating probabilities and risk, using examples of misleading statements, might give people the tools to discredit false calculations/claims and needed scepticism about 'fake news' of all kinds. Some police and government interviewees in 2021–2022 referred to campaigns around seatbelts and smoking (or even switching off cell phones in cinemas and theatres) as examples of successful Protect efforts. But this analogy from static risks underplays the challenges in transferring risk awareness between different contexts and techniques, for example, associating abstract information with the situational dynamics of social engineering, whether direct (e.g., during affinity and romance frauds) or largely generic and online. Warnings alone have little impact (Kamar et al., 2022). Mock 'stings' have seldom been used to warn people how easily they could have been scammed, perhaps because of public relations fears by police and banks. One might expect some University ethics committees to object to such experiments conducted by academic researchers.

Interventions by charities and regulators aim at impacting potential fraud victims, including banning cold calling without prior requests from clients.[23] The proportion receiving one or more unsolicited approaches fell in 2021–2022 (FCA, 2023), but a longer follow-up is needed to test if this was due to a 2019 ban on cold calling about pensions. 62% of consumers proceeded to transfer their private pensions to scammers even when warned of the risks (Skidmore, 2020): a challenge for opponents of the paternalist model. Department of Work and Pensions Regulations use amber and red warning flags to inhibit them before transfers from company pensions are allowed.[24]

Advertising campaigns

The rise of Google and Meta marketplace and other digital promotion venues has gradually stimulated proactive monitoring and interventions. There have been many efforts by third sector, banks and police in the UK to promote education to the public on how to protect themselves against fraud, but data and methodology on impacts remain unpublished. Some academic experiments (Bekkers et al., 2024; Jensen et al., 2024; Kamar et al., 2022; Moneva and Leukfeldt, 2023) and discussion papers (Drew and Farrell, 2018) offer insights, but on the assumption that many supply-side online (and offline) fraud prevention attempts will fail to stop many people receiving *some* fraudulent

offers, protection by self, family and friends (if any) and by commercial and not-for-profit third parties seems essential if harm is to be reduced substantially.

COVID-19 provided a significant impetus for UK efforts at warnings to members of the public, since there was a well-founded fear that scammers would exploit the pandemic. The National Cyber Security Centre (NCSC) has cybersecurity infographics into which a lot of effort has been put,[25] whose targets are individuals, families and small businesses, large corporations and cybersecurity professionals: but people need to be motivated to actively consult the websites (Collier et al., 2022). UK police and banks have issued warning adverts, under the 'Take Five' (minutes to reflect) umbrella, paid for by the banks: these vary in the degree to which they take account of social engineering and crime scripts. It seems unlikely that all romance fraud targets will realise that 'Swipe left for romance fraud' applies to their situation, even if they have seen and remembered the advert.[26] The Financial Conduct Authority has paid for warnings about crypto investments and the need to check that financial advisers are authorised; they use social media to warn the public, mainly against Influencers. Although they continue to host many scam advertisements, Google and Meta have agreed (after some years) not to take advertisement business without first checking that firms claiming to be authorised by the regulators actually are.[27] The UK government launched in February 2024 and March 2025 some adverts on social media, television, radio and press aiming to alter general perceptions of risk and make people more cautious.[28] We do not yet know what impacts (and on what fraud types) these campaigns may have had, or what impacts more repeat victim-targeted campaigns might have.

Reduce victimisation of vulnerable persons and repeat victimisation

The distribution of both frauds and repeated frauds is uneven, as is the case for other crimes. Repeat attempts by the same offenders and the sharing of data on victims between offenders increases risks to the public, as do deep fakes, and this is a nuisance even if unsuccessful, and very harmful if successful. One approach to prioritisation of interventions with very scarce resources is to focus on 'vulnerable' and on repeat victims, which overlap (Cross, 2016). There are potential links of fraud into the adult safeguarding regime of police and local authorities (Olivier et al., 2016), but contemporary criminological research does not consider it (Crawford, 2024).

Definitions of vulnerability tend to be imprecise: the UK National Vulnerability Action Plan (NPCC, 2022) mentions cyber and elder abuse but not fraud, and states 'A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves or others from harm or exploitation.' An ageing population, smaller family sizes and decline in people available to help, plus AI-assisted deep fakes and other changing technologies will mean more people potentially will be 'unable' to protect themselves in this way, in many parts of the world. But vulnerability can mean either the statistical chance of becoming a single/repeat victim or being specially harmed if one is victimized, and folk beliefs rather than evidence may guide interventions.

In 2022–2023, 1 in 10 surveyed fraud victims were victimised two to four times and 1 in 100 more than four times (ONS, 2023b: Table D7). One in 20 consumer and retail

fraud victims were victims more than once, but a higher percentage of *non*-cyber fraud (11%) than of cyber-fraud (8%) victims were repeat victims (Table D8).[29] Taking the Action Fraud 18% repeat victim figure in the Home Office (2023) National Fraud Strategy, help for repeat victims would require managing the risks and support for some 60,000 people, or (including non-reporting ONS Crime Survey numbers) nearly 800,000 people annually. The West Midlands data show that two-fifths of those reporting fraud have been fraud victims before in their lifetimes: half or more in the Action Fraud categories Fraud by Abuse of Position, Retail Fraud, Door to Door Sales and Bogus Traders, and Cheque, Plastic Card and Online Bank Accounts were repeat victims (Levi et al., 2023). Among repeat victims meeting the criteria for highly vulnerable, the most common fraud categories are Time Shares and Holiday Club Fraud, Other Financial Investment and Dating Scams. But historic data do not enable us to distinguish 'repeats' for the same type of fraud, from any fraud at all, the frequency and rapidity of the victimisation, or multiple losses within the same scam. Especially if we include the almost half the adult UK population who have 'characteristics of vulnerability', help at scale would require enormous resources.[30] Where might those resources come from?

Banks keep registers of account holders who they deem 'vulnerable' (whether or not repeat victims) and who are to be questioned if they try to take out large amounts of cash or transfer large funds to strangers. The Banking Protocol 2017 – extended in 2020 – is an agreement with the police for banks to call them to attend when bank staff are suspicious, to assist in stopping customers from handing over money to 'courier fraudsters'. Nationally, the emergency procedure was used 11,643 times in 2022, leading to savings of £55 million and almost 200 arrests, though a senior officer interviewed in the West Midlands Economic Crime Unit said he knew of no such calls to his colleagues for support to it.[31] Account-holder reactions are not collated or published. The company trueCall provides a generic service, but also works with Trading Standards officers: If the caller is trusted (pre-listed by the consumer), then the phone rings as normal, but if it is an unrecognised caller, trueCall intercepts the call and plays them a message. For example: 'Hello – if you're a friend, family member or invited caller please press "1", if you are a cold caller please hang up and don't call again'. Data show that this has an impact on victimisation of 'vulnerable people' (Passenger, forthcoming). However, it can increase isolation among those with no or few relatives and friends.

Repair the well-being of distressed victims

The provision of emotional support and restorative justice for fraud and other victims is a social objective in itself, irrespective of impacts on repeat victimisation. There is little information in many countries about support different sorts of fraud victims receive. The National Economic Crime Victim Care Unit began as a very small team of former officers in the City of London Police (Author interviews, 2015; Home Office, 2025) but has expanded to cover all UK force areas. It provides levels of service reflecting the assessed vulnerability of each victim. Level 3, for the most vulnerable, takes a multi-agency approach. 'Of those using the NECVCU services, only 0.03% were the victims of a subsequent online fraud. That compares with CSEW data suggesting that 13% of all fraud victims have been victimised more than once'.[32] Realistically, given the millions

of victims and repeat victims, its 2024 staffing of 43 does not have capacity to offer a significant service to many victims, nor is it obvious that this should always be a *police* function: though AI may generate more relevant advice to victims than did past standardised offerings, it is not a likely source of emotional reassurance and repair, especially for the cognitively impaired (a dynamic state for some) and for those who do not access the Internet.

An array of Third Sector charities assist fraud victims in the UK. Earlier decades of the victims' movement *assumed* that fraud victims were not appropriate or priority recipients of intervention (Levi and Pithouse, 1992). Victim Support – which assisted almost 5000 fraud victims in 2022 – has not included a strongly evidence-based crime *prevention* strategy hitherto. Victim Support (2022: 11) states:

> We help those who have been defrauded by ensuring they are safe, informed and advised about their rights and entitlements. We also provide support to recover from the impacts of fraud, and ensure that victims are connected to the people and networks that will help prevent future fraud. We also support people to share their experiences with others in order to raise awareness and educate about the dangers of fraud.

Its Annual Reports contain many references to fraud, and its website now contains quite comprehensive material, with further links and help guides on online frauds (but not offline, e.g., affinity and doorstep frauds) for those who register.[33] The Age UK (2024) Lloyds Banking Group-funded Scams Prevention and Support Programme offers a range of services, for example, 4979 older people during 2022 and 2023 had bespoke one-to-one support sessions and 25,850 participated in awareness talks. While noting the difficulties of cognitive decline for recall, there were some confidence- and competence-enhancing effects, and their programmes will be further developed. Citizens' Advice nationally has awareness campaigns and helpful resources. In addition to scam alerts for which people can sign up, there is a broad campaign by Which? magazine to combat scams.[34] There is no information yet on the impacts of these other interventions (see Button et al., 2024).

The term 'vulnerability' would benefit from more careful exploration 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. Victim support measures would require rigorous trial evidence of impacts on, say, anxiety, health or repeat victimisation to be considered a core part of any scientific public health approach.

Reduction in 'unproductive' fear of fraud

Cook et al. (2023) and Guedes et al. (2025) have highlighted high fear of cybercrime and cyber-related frauds in Europe. However, fears have functional as well as dysfunctional effects, in making us distrust people and what they say and write, and sometimes that protects us. Some might argue that every fraud victim has got this trust balance wrong, though outcomes that exclude good offers foregone are only partial measures of rationality in risk-taking. One of the many challenges in a public health model is to find a balance between productive and unproductive fears. There is an increasing literature

on fear of fraud – especially among older people – but it generally treats fear as something self-evidently to reduce rather than sometimes to use constructively.

Discussion: Counter-fraud interventions

Public health approaches include police and non-police interventions supported by evidence of effectiveness normally generated in rigorous randomised trials or quasi-experiments, though in a fraud and cybercrime context, 'realist evaluations' of context-mechanism-outcome can be a more viable and valuable alternative. Notwithstanding a large array of experimental policing studies of offline crimes including tax compliance (Ariel, 2012), such experiments (and double-blind trials generally) involving decisions *not to* prevent frauds among a control group might be a challenge for public relations departments in business, policing and university sectors: non-intervention in the control group is not actively doing harm, but it clearly involves deciding not to prevent or reduce harm in the current case, and banks and other businesses may be afraid of media criticism, whatever the strategic 'health' benefits of evidence-based fraud control. Few criminologists have the prestige of medical professionals, nor are there the vast financial benefits to providers from government drug or machine licensing to induce classical methodological conformity. Furthermore, to the extent that public health approaches have enjoyed success, it has usually been in the context of highly visible violent crimes, whose harms are manifest to doctors who treat them, or of diseases that have been analysed in laboratories and can be attributed to failures of public sanitation, et cetera. Frauds are manifested in loss of income, emotional distress, and loss of trust and mental capacity. Given general societal demand strains upon mental health professionals – aggravated by COVID-19 – there is little space among medical professionals for fraud symptoms and treatment. We need to be realistic about the paid-for and voluntary community resources that can be deployed to support fraud victims and potential victims.

'Effectiveness' can depend on our time horizons, and activities that may provide public and media reassurance may have far less impact on future offending levels, while other efforts may be abandoned if they do not show quick results (Tilley, 2024). A Scottish Government/EKOS Limited (2021: 9) review of financial scam costs noted the absence of serious evaluations, and this also applies to many promising interventions in the annual UK Tackling Economic Crime Awards.[35] Arguably, to keep initiatives going, they need support that cannot wait for sober evaluation perhaps years later. Randomised Controlled Trials and quasi-experiments, or even 'realistic evaluations', are rare in counter-fraud initiatives. To the extent that commitment, cooperation and charisma (or their absence) affect success, the failure to measure these inputs is a methodological weakness in such evaluations. There may also be a publication bias from public and private bodies themselves in favour of positive results. By Q2 2025, no results from public awareness campaigns have been published by banks or by government.Whatever the symbolic importance of criminal law, given the number and range of frauds and victims, an enforcement-*only* response is not a feasible option for fraud control even in mandatory prosecution systems like Austria, Germany and Italy. Protect and Prepare measures have been highlighted as a route to individuals' fraud reduction, though the police and Trading Standards are constrained (for anti-corruption reasons) from recommending particular products, and unlike NCSC, they may not possess sufficiently specific

skills for the high end fraud or cyber risks. The police.uk website in 2023/2024 referred users to GetSafeOnline and to CyberAware websites for prevention advice: until 2023 updates, the only other specific fraud advice was for Muslims on avoiding Hajj fraud.

Another strand for consideration is the extent to which the police can and should investigate economic cybercrimes that have international dimensions where suspects are out of practical reach: though there might still be a case for efforts to enhance victim satisfaction and care, and political relationships can change, early decisions on this could save scarce resources being wasted. But if begun early enough, criminal investigations can freeze proceeds and enable them to be recovered for victims, and proactive Regional Organised Crime Units and other teams can reduce the numbers and harms to victims even if no convictions ensue. Civil litigation can do this too, but costs too much for most victims. Where law enforcement interventions can arrest offenders and disrupt cybercrime markets, or where the policing or private/third sector body takes down websites, their disruptive effects can be short term (Bergeron et al., 2020; Décary-Hétu and Giommoni, 2017; Goonetilleke et al., 2023), but they may have some positive impact on deterrence and on police legitimacy. The UK NCSC has become increasingly active,[36] and manages the takedown service centrally.

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, if the evidence shows health improvement as a result of defined interventions. One of the motivations for a public health approach is to encourage bottom-up as well as top-down efforts at fraud harm reduction, but there are many practical challenges in motivating civil society parties to action, especially when education, mental health and financial intervention services as well as policing and crime victim support services face severe austerity pressures.[37] A focus on equalities of care for fraud victims would repay the attention of European policy-makers.

Concluding comments

Most traditional 'white-collar crime' scholars still pay little if any attention to volume scams, which fall uneasily between white-collar crimes and organised/networked criminality and also do not fit readily into 'crimes of/by capitalism'. Many industry responses to fraud form part of the extension of crime control beyond the State and legally mandated private sector 'responsibilisation' (Garland, 1996) that we see also in the Anti-Money Laundering arena, though with more tangible effects on crime than money laundering controls have been shown to provide (see e.g., Halliday et al., 2020). Routine activities theory (RAT) and situational crime prevention revolve around 'motivated' offenders, 'suitable' victims and 'capable' guardians, and this article has noted how flexible a range each component connotes. More people can become motivated offenders if they realise how crimes can be accomplished and are offered easy tools that reduce the skill barriers to entry, such as 'crime-as-a-service' kits or cheap companies to use as fronts for scams (Europol, 2024, 2025). AI has already eased fakery of voice and face recognition, changing 'what works' in individual and corporate guardianship such as voice recognition for banking apps. A large proportion of the population are already 'suitable' victims for *some* offenders and for some types of fraud. In different parts of the world,

guardianship can be more or can be less capable (and capacitated) for particular types of frauds, inside and outside the legal perimeter of regulators or the *de facto* interests and priorities of national and international police bodies. Holt et al. (2020) and Williams (2016) have already used RAT creatively for cyber-dependent crimes and identity theft, and use of it for other frauds should stress the flexibility of its constituent parts. But academics and policy-makers should note that there are other frauds involving harmful *corporate* actors which have different logics and control strategies (Lord and Levi, 2025): they would require a different 'public health' approach and muscular politics to mitigate.

It is reasonable to ask what difference it makes to badge strategies as 'public health' rather than crime control, crime reduction, multi-agency policing or 'holistic' ones. The term 'public health' intentionally expresses the view that protecting broad swathes of the public from psychological and financial harms – however achieved – is the key goal, and the mechanism for reaching it is institution-neutral. As in 'reassurance policing', public health goals might include emotional repair and fear reduction as well as actual fraud reduction. However, there is no reason to suppose that such approaches will always be successful, either generally or in relation to any type(s) of fraud, and evidence is not currently good enough to put its role in countering fraud into more than a 'promising' category. The label of public health does not *per se* create any more resources, unless specific 'command' powers are attached to it. Integrated Health Boards and others allocating resources in the UK or elsewhere might consider the mental health impacts of some frauds and put fraud victimisation on the mental map of service providers, and the West Midlands Fraud Board is pursuing a range of actions. The Police Foundation (2022) recommends a non-police-led Crime Prevention Agency as a way of focussing thinking, and combating frauds and cybercrimes should be a significant component of that. Although knowledge of finance does not confer immunity from fraud, there is also a need to improve financial literacy, a component of which might be the UK opting into the OECD's Pisa evaluation for financial literacy.[38]

A step change towards achieving better outcomes would be more targeted behavioural interventions including those on victims or via third party interveners. The FCA has begun this (Delias et al., 2022; Farghly et al., 2022; FCA, 2024), but it needs greater qualitative insights. We can learn from failed attempts on what people do to avoid becoming victims, and classify frauds more usefully than Action Fraud has done so that we can assess how they are changing, bearing in mind psychological reactance issues such as individuals' resistance to 'rational' advice (Dove, 2020) and fraudsters' social engineering skills (Carter, 2023). Identifying those particularly likely to be defrauded – and appreciating that life events such as redundancy (especially with a large payout), family death or divorce can expose people to particular risks – is a stage towards more evidence-based targeted interventions. So too is becoming a victim, which may generate a 'teachable moment' when we are most likely to be able to learn how to avoid some or all frauds. Both the implementation and impacts of interventions would benefit from market testing field experiments of a kind sometimes done on the efficacy of anti-money laundering processes (Findley et al., 2025). The magazine Money Which?, journalists and trading standards officials sometimes do this to test claims of compliance by private and public sectors alike: see, more generally, Lord and Levi (2024).

This article has not had the space to deal specifically with fear of fraud in Europe or elsewhere, but fears *can* be a stimulus to self-protection. There will remain tensions over the extent to which people should be pressurised/actually prevented from becoming victims of fraud, especially where the financial intermediary has to compensate them. But this is no less true of other areas of public health like diet where costs and benefits have to be traded off. Although there are remnants of victim-blaming in media accounts and public attitudes, the voluntary handing over of money by victims under false beliefs about the integrity and means of recipients – whether agents or principals – has already moved substantially in the cultural dial from Victorian expectations of prudence. There remain legitimate questions about the limits of victim entitlement to compensation when they have disregarded explicit warnings and lied to banks. The UK government has sought to pressurise businesses into compliance via regulatory requirements and, in some cases, via voluntary Fraud Charters, in the attempt to 'Make Financial Polluters Pay'. Reasonable people can differ about the proper limits of (ir)responsibility among those who lose money to fraudsters and about when victims are morally and/or legally entitled to be compensated. Social, legal and technical controls constitute collectively an ongoing dynamic whose impacts on levels and patterns of fraud will need careful exploration and funding. Scholars, policy-makers and practitioners might consider broader collective efficacy frameworks that include the impacts of widespread unpunished fraud at home and abroad, and continue the search for protective and restorative interventions that marshal and amplify the efforts of all potential guardians.

Author note

Michael Levi has received lifetime research awards from the American, British and European Societies of Criminology for his contributions to organised and white-collar crimes and their control.

Acknowledgments

Thanks to Ben Collier and to the reviewers for their helpful comments. I am grateful to Alan Doig, Jodie Luker, Matthew Williams, and Jonathan Shepherd for their work on the original West Midlands study. That study benefited particularly from the support of West Midlands Police and Crime Commissioner Simon Foster; former policy officer Brendan Warner-Southwell; current Deputy PCC Wasim Ali and former Deputy PCC Waheed Saleem; Wayne Haynes, formerly of the West Midlands Regional Organised Crime Unit; Kuldeep Maan and Christopher King of Dudley Trading Standards; and Alex Pritchard and colleagues at the West Midlands police. I am also grateful for insights from staff at the City of London police, the National Crime Agency, the National Cyber Security Centre, the Serious Fraud Office, National Trading Standards, the MASH teams, and to Andrew Passenger of Carmarthenshire Trading Standards, as well as some Dutch, Europol and other European police and staff at the European Commission.

Data availability

The raw data are classified, but general demographic material on fraud victims are available in the research reports at https://www.westmidlands-pcc.gov.uk/preventing-crime/fraud/.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval

This study was granted ethical approval by the Cardiff University SOCSI Ethics Committee.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The West Midlands Office of the Police and Crime Commissioner, the West Midlands Regional Organised Crime Unit, and the Midlands Fraud Forum co-funded the original study from which this work has been developed; the British Academy funded the COVID-19 fraud research SRG20\201612.

ORCID iD

Michael Levi https://orcid.org/0000-0003-2131-2882

Notes

1. Although there remain many large and impactful frauds whose cyber assisted or enabled component is restricted to emails and electronic fund transfers, the terms 'cyber assisted' and 'cyber-enabled' (McGuire and Dowling, 2013; Wall, 2024) fraud have lost much analytical value because of technological changes in the financial sector and the inclusion of money laundering in thinking about the organisation of most crimes for gain. Few – mainly older – people now have landlines, so many phone calls and all spoofed numbers are 'cyber enabled'. Currently, 48% of frauds are flagged as cyber in the England and Wales crime survey (ONS, 2025b), *proportionately less* than that reported in 2016–2020: 'Cyber fraud represents cases where the internet or any type of online activity was related to any aspect of the offence'. In a motivational examination of cybercrimes and the cyber/fraud overlap in Nigeria, Ibrahim (2016) opts for the term 'socioeconomic cybercrimes'. Some official press notices embody this conceptual confusion: for example, should setting up dummy companies on computer software for insider embezzlement really be filed initially under 'FBI cyber news'? See https://www.justice.gov/usao-ndil/pr/former-chief-financial-officer-chicago-hospital-among-three-defendants-charged-alleged.
2. For a more developed version, see https://assets.college.police.uk/s3fs-public/2021-09/policing-and-health-collaboration-landscape-review-2021.pdf: fraud does not appear in this landscape.
3. Although sample size was only 2000 per country.
4. Vehicle related theft, domestic burglary, theft from the person and robbery of personal property (Home Office, 2021).
5. All UK parties before and during the 2024 election campaign mentioned clamping down on tax evasion and avoidance to pay for public services. The Conservative party manifesto (2024: 22) mentioned only welfare fraud, but the 2024 UK Labour Party manifesto (https://labour.org.uk/change/take-back-our-streets/), Liberal Democrat manifesto and – more strongly – their Scottish versions did propose a range of actions against those frauds impacting consumers.

6. https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024.
7. The *Guardia di Finanza* have long had an important role, but the *Polizia Postale* now have a cybercrime team.
8. German Code of Criminal Procedures. 152(2): [The public prosecutor] is required to take action against all judicially punishable … acts, to the extent that there is a sufficient factual basis. The number of German fraud investigations went down from 982,000 in 2017 to 928,000 in 2022, and some 130,000 were convicted of fraud type-offences. For data on recorded economic crime in Germany, see https://www.bka.de/SharedDocs/Downloads/EN/Publications/PoliceCrimeStatistics/2024/pks2024CasesBasicTable_excel.xlsx?__blob=publicationFile&v=4.
9. Three quarters in unpublished City of London police estimates, though this figure should be treated with caution.
10. https://www.westmidlands-pcc.gov.uk/pcc-launches-new-approach-to-tackle-fraud-in-west-midlands/; https://www.westmidlands-pcc.gov.uk/pcc-highlights-devastating-impact-of-fraud-and-vows-to-take-action/.
11. Author research; see also https://www.cityoflondon.police.uk/police-forces/city-of-london-police/areas/city-of-london/about-us/about-us/national-lead-force/.
12. Some guardians are more capable (and willing) than others at any one time or in adapting to changing threats, so the term 'capable guardians' is too binary and static.
13. Not for profit fraud prevention body Cifas is the most active third sector body in the UK.
14. These compel banks and other payments companies to reimburse customers who fall victim to APP fraud – see for example, https://www.wearepay.uk/app-authorised-push-payment-reimbursement-policy/ – reduced to £85,000 after strong lobbying. In 2023, different UK banks fully reimbursed between 9% and 89% of losses by value, and between 3% and 96% of losses by volume of cases (PSR, 2024).
15. The Foreword to the UK Finance (2024: 7) fraud report and its letter (with *Which?)* to the government in March 2025 demand faster implementation of controls on social media. For US parallels and data, see https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers.
16. https://www.thisismoney.co.uk/money/beatthescammers/article-12828093/VICTORY-Social-media-giants-finally-promise-crack-scammers-Campaign.html. How realistic the threat of firmer action actually is and is perceived to be (and by whom) is a matter of judgment. Such pressures also exist in other countries, though the Trump administration support for US tech companies makes it challenging to crack down on them.
17. For a sample of national approaches, see, for example, https://www.cifas.org.uk/; https://www.gasa.org/; https://fintrail.com/; https://www.accc.gov.au/national-anti-scam-centre; https://antifraudcentre-centreantifraude.ca/index-eng.htm.
18. Irvin-Erickson (2024) is right to separate out id *thefts* from id *frauds*, but identity thefts are often not thefts in the zero-sum way that most thefts are: 'illegal identity appropriation' might be a more accurate term, since identities are *duplicated* rather than entirely removed from the original owners, who nevertheless subjectively may *feel* that their identities have been 'stolen'.
19. From 34.5 million SERs received, 351,000 scam URLs were removed by the National Cyber Security Centre April 2020–24 as part of the Active Cyber Defence (NCSC, 2024). In March 2024, more than 60,000 malicious websites were removed as a result of being reported using [free text] 7726. (https://www.actionfraud.police.uk/news/phishing – accessed 21 July 2024).

20. Frauds are the *only* crimes for gain where reports cannot be made locally to UK police forces. An unintended consequence is that people cannot currently be provided by www.police.uk with contemporary data on levels of recorded fraud in their area (see https://www.actionfraud.police.uk/data). It is unclear how important that might be.
21. https://apnews.com/article/thailand-myanmar-scam-electricity-cut-0cfdfb57aa2e05e5835b1af3b4ac8e1a.
22. https://www.biocatch.com/blog/faster-payments-sand-in-the-gears; Payment Services (Amendment) Regulations 2024.
23. ScamSmart resources|FCA.
24. https://www.gov.uk/government/consultations/pension-scams-empowering-trustees-and-protecting-members/pension-scams-empowering-trustees-and-protecting-members-consultation; *Which? Money*, January 2022. https://www.thepensionsregulator.gov.uk/en/document-library/research-and-analysis/pension-scams-threat-assessment-summary.
25. https://www.ncsc.gov.uk/information/infographics-ncsc#section_1.
26. https://www.takefive-stopfraud.org.uk/supporters-campaign-materials/.
27. If the social media firms were regulated for money laundering, it would be an offence to take money for advertising that came from crime. Even without such regulation, it may be an offence to do so knowingly or recklessly.
28. StopThinkFraud (https://stopthinkfraud.campaign.gov.uk./). All of the (young to middle aged) people featured on the website were using web tech – phones, tablets and laptops.
29. 'Non-cyber' represents offences which did not involve the internet or any online activity; 'Cyber' represents cases where the internet or any type of online activity was related to any aspect of the offence.
30. https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers.
31. https://www.bbc.co.uk/news/business-66165920.
32. https://www.crestadvisory.com/post/tackling-online-fraud-what-do-the-experts-think, though neither numbers nor periods of follow up are given. From April 2019 to January 2020, the service provided support to 4,378 London victims over the phone and provided an additional 5,694 victims with fraud prevention advice either by post or email. https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/economic-crimevictim-care-unit. These are process data that do not examine impacts.
33. https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime/; https://www.victimsupport.org.uk/crime-info/types-crime/fraud/.
34. https://www.which.co.uk/campaigns/stampout-scams.
35. https://thetecas.com/. There is a range of individual and team categories.
36. http://www.ncsc.gov.uk/information/takedown-service.
37. Allocation of support funds from proceeds of fraud confiscation – net of compensation – might be possible: see Levi et al. (2023) for UK confiscation and compensation data. But confiscated assets in England Wales are currently allocated annually for projects, not as core funding for longer term needs or for social prevention programmes as in Scotland.
38. See, for example, https://www.cifas.org.uk/insight/public-affairs-policy/anti-fraud-lesson-plans.

References

ABA (2024) *Extra Care for Customers Experiencing Vulnerability*. Sydney: Australian Banking Association.

Aebi M, Miro-Llinares F and Caneppele S (eds) (2025) *Understanding Crime Trends in a Hybrid Society: The Digital Drift*. New York: Springer.

Ariel B (2012) Deterrence and moral persuasion effects on corporate tax compliance: Findings from a randomized controlled trial. *Criminology: An Interdisciplinary Journal* 50(1): 27–69.

Arnot J and Mackie P (2019) *Scottish public health network violence prevention framework*. Glasgow: ScotPHN.

Bekkers LM, Moneva A and Leukfeldt ER (2024) Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology* 20(2): 375–394.

Bergeron A, Décary-Hétu D and Giommoni L (2020) Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy* 83: 102870.

Birkel C, Church D, Erdmann A, et al. (2020) *Sicherheit und Kriminalität in Deutschland – SKiD 2020*. Berlin: BkA.

Bowling B, Reiner R and Sheptycki J (2019) *The Politics of the Police*, 5th edn. Oxford: Oxford University Press.

Brå (2024) The Swedish Crime Survey 2024. Available at: https://bra.se/english/publications/archive/2024-10-16-swedish-crime-survey-2024.

Brewer R, de Vel-Palumbo M, Hutchings A, et al. (2019) *Cybercrime Prevention: Theory and Applications*. New York: Springer Nature.

Button M (2021) Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a national economic crime agency. *Policing: A Journal of Policy and Practice* 15(3): 1758–1772.

Button M, Hock B, Shepherd D, et al. (2023) Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology* 1: 100012.

Button M, Karagiannopoulos V, Lee J, et al. (2024) Preventing fraud victimisation against older adults: Towards a holistic model for protection. *International Journal of Law, Crime and Justice* 77: 100672.

Carter E (2023) Confirm not command: Examining fraudsters' use of language to compel victim compliance in their own exploitation. *The British Journal of Criminology* 63(6): 1405–1422.

Collier B, Flynn G, Stewart J, et al. (2022) Influence government: Exploring practices, ethics, and power in the use of targeted advertising by the UK state. *Big Data and Society* 9(1): 1–13.

Collier B, Stewart J, Horgan S, et al. (2023) *Influence Policing: Strategic Communications, Digital Nudges, and Behaviour Change Marketing in Scottish and UK Preventative Policing*. Edinburgh: Scottish Institute for Policing Research.

Collier B, Thomas DR, Clayton R, et al. (2019) Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. In: Proceedings of the internet measurement conference, pp. 50–64. October 21-23, Amsterdam, the Netherlands.

CoLP (2023) National policing strategy for fraud, economic and cyber crime 2023–2028. Available at: https://www.cityoflondon.police.uk/police-forces/city-of-london-police/areas/city-of-london/about-us/about-us/national-lead-force/.

Cook S, Giommoni L, Trajtenberg Pareja N, et al. (2023) Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. *British Journal of Criminology* 63(2): 384–406.

Crawford A (2024) Vulnerability and policing: Rethinking the role and limits of the police. *The Political Quarterly* 95(3): 431–441.

Cretu-Adatte C, Azi JW, Beaudet-Labrecque O, et al. (2024) Unravelling the organisation of Ivorian cyberfraudsters: Criminal networks or organised crime? *Journal of Economic Criminology* 3: 100056.

Cross C (2016) Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Criminal Justice Studies* 29(2): 125–142.

Cross C (2020) Responding to individual fraud: Perspectives of the fraud justice network. In: Leukfeldt R and Holt TJ (eds) *The Human Factor of Cybercrime*. Abingdon, Oxon: Routledge, 359–388.

Décary-Hétu D and Giommoni L (2017) Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation Onymous. *Crime, Law and Social Change* 67(1): 55–76.

Delias D, Farghly F, Hayes L, et al. (2022) *Going beyond 'Capital at Risk': Behaviourally Informed Risk Warnings for High-Risk Investment Products*. London: Financial Conduct Authority.

Doig A, Levi M and Luker J (2025) 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. *Security Journal* 38(1): 1–33.

Dove M (2020) *The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable*. London: Routledge.

Drew JM and Farrell L (2018) Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research* 19(6): 537–549.

Dudink Y, Taminiau Y and Veenswijk M (2023) The dark side of public-private partnerships: Enforced hybridity and power dynamics in fighting financial crime. *Public Policy and Administration* 39(3): 497–518.

Dupont B (2019) The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity* 5(1): 1–17.

EBA (2024) *2024 Report on Payment Fraud*. Frankfurt: European Banking Authority.

Europol (2024) *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxembourg: Publications Office of the EU.

Europol (2025) *EU Serious and Organised Crime Threat Assessment 2025*. Luxembourg: Publications Office of the EU.

Farghly F, Hayes L, Ng C, et al. (2022) *Pausing, Reading, and Reflecting: Decision Points in High-Risk Investment Consumer Journeys*. London: Financial Conduct Authority.

FCA (2023) *Financial Lives Survey*. London: Financial Conduct Authority.

FCA (2024) *Business Plan 2024/25*. London: Financial Conduct Authority.

Findley M, Nielson D and Sharman J (2025) Banking bad? A global field experiment on risk, reward, and regulation. *American Journal of Political Science* 69(2): 545–559.

Garland D (1996) The limits of the sovereign state: Strategies of crime control in contemporary society. *The British Journal of Criminology* 36(4): 445–471.

GASA (2024) Global state of scams report 2024. The Hague: Global anti-scam alliance.

Goonetilleke P, Knorre A and Kuriksha A (2023) Hydra: Lessons from the world's largest darknet market. *Criminology & Public Policy* 22: 735–777.

Guedes IS, Martins J and Moreira S (2025) Explaining fear of cybercrime: A focus on interpersonal and property cybercrime differences. *European Journal of Criminology*: 14773708241312820.

Halliday T, Levi M and Reuter P (2020) Why do transnational legal orders persist? The curious case of anti-money laundering. In: Shaffer G and Aaronson A (eds) *Transnational Legal Ordering of Criminal Justice*. Cambridge: Cambridge University Press, 51–83.

HMICFRS (2024) *State of Policing: The Annual Assessment of Policing in England and Wales 2023*. London: Home Office.

Holt TJ, van Wilsem J, van de Weijer S, et al. (2020) Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review* 38(2): 187–206.

Home Office (2021) *Beating Crime Plan*. London: Home Office.

Home Office (2023) *Fraud Strategy: Stopping Scams and Protecting the Public*. London: Home Office.

Home Office (2025) *Experiences of Victims of Fraud and Cyber Crime*. London: Home Office.
Hyde R and Gibson J (2024) *It's a Fraudster's World: Exploring the Scale, Impact, and Globally Interconnected Nature of Fraud against Consumers*. London: Social Market Foundation.
Ibrahim S (2016) Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice* 47: 44–57.
Ilbiz E and Kaunert C (2023). *The Sharing Economy for Tackling Cybercrime*. New York: Springer.
Irvin-Erickson Y (2024) Identity fraud victimization: A critical review of the literature of the past two decades. *Crime Science* 13: 3.
Jensen RIT, Gerlings J and Ferwerda J (2024) Do awareness campaigns reduce financial fraud? *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-024-09573-1.
Kamar E, Howell CJ, Maimon D, et al. (2022) The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and SMiShing victimization: An experiment. *Justice Quarterly* 6: 837–858.
Levi M (2006) The media construction of financial white-collar crimes. *British journal of criminology* 46(6): 1037–1057.
Levi M (2008) *The Phantom Capitalists*, 2nd edn. London: Routledge.
Levi M (2010) Public and private policing of financial crimes: The struggle for co-ordination. *Journal of Criminal Justice and Security* 12(4): 343–357. https://www.fvv.um.si/rv/arhiv/2010-4/Levi.pdf.
Levi M (2022) Fraud, pandemics and policing responses, SPECIAL CONFERENCE EDITION Nr. 5 Pandemic effects on law enforcement training & practice: Taking early stock from a research perspective, 23–29. Available at: https://op.europa.eu/en/publication-detail/-/publication/5a5afa91-7e5e-11ec-8c40-01aa75ed71a1/language-en.
Levi M (2023) Frauds in digital society. In: Housley W, Edwards AE, Beneito-Montagut R and Fitzgerald R (eds) *Sage Handbook of Digital Society*. London: Sage, 480–500.
Levi M, Bissell P and Richardson T (1991) The prevention of cheque and credit card fraud. CPU Paper No. 26. London: Home Office.
Levi M, Doig A, Gundur RV, et al. (2017) Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change* 67(1): 77–96.
Levi M, Doig A, Luker J, et al. (2023) Towards a public health approach to frauds, Office of Police and Crime Commissioner, West Midlands, UK. Vols. 1 and 2. Available at: https://www.westmidlands-pcc.gov.uk/fraud/.
Levi M and Handley J (1998) The prevention of plastic and cheque fraud revisited. Home Office Research Study No. 182. London: Home Office.
Levi M and Maguire M (2004) Reducing and Preventing Organised Crime: An Evidence-based Critique. *Crime, Law and Social Change* 4(Juune): 397–469.
Levi M and Pithouse A (1992) Victims of fraud. In: Downes D (ed) *Unravelling Criminal Justice*. London: Macmillan, 229–246.
Lord N and Levi M (2024) *Organising White-Collar and Corporate Crimes*. London: Routledge.
Loveday B and Jung J (2021) A current and future challenge to contemporary policing: The changing profile of crime and the police response. Examples of policing fraud in two police jurisdictions: England and Wales and South Korea. *Policing: A Journal of Policy and Practice* 15(3): 1633–1650.
Mcguire M and Dowling S (2013) Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Office Research report* 75: 1–35.
Meerts CA, Huisman W and Kleemans ER (2025) Living apart together: Public-private cooperation in the field of financial crime. *Crime, Law and Social Change* 83(18): 1–21.

Moneva A and Leukfeldt R (2023) The effect of online ad campaigns on DDoS-attacks: A cross-national difference-in-differences quasi-experiment. *Criminology & Public Policy* 22: 869–894.

Na C (2023) Proactive crime prevention through problem-oriented governance: A case study of South Korea's recent efforts to tackle new types of fraud. *Policing: A Journal of Policy and Practice* 17: paac080.

NCSC (2024) NCSC annual review 2024. Available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024.

Newburn T (2024) *The Official History of Criminal Justice in England and Wales Volume V: Policing Post-war Britain: Plus ça change*. London: Routledge.

NPCC (2022) *UK National Vulnerability Action Plan*. London: National Police Chiefs Council.

Ofcom (2023) Online frauds and scams. Available at: https://www.ofcom.org.uk/online-safety/online-fraud/online-fraud-and-scams/.

Ofcom (2024) Experiences of fraud online and through calls and texts. Available at: https://www.ofcom.org.uk/online-safety/online-fraud/online-call-and-text-fraud/.

Olivier S, Burls T, Fenge LA, et al. (2016) Safeguarding adults and mass marketing fraud–perspectives from the police, trading standards and the voluntary sector. *Journal of Social Welfare and Family Law* 38(2): 140–151.

ONS (2023a) Crime in England and Wales: Year ending June 2023. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2023.

ONS (2023b) Crime in England and Wales, annual trend and demographic tables – Year ending March 2023. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023#:~:text=2.-,Overall%20estimates%20of%20crime,2020%20(10.2%20million%20offences).

ONS (2025a) Crime in England and Wales: Year ending September 2024. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2024.

ONS (2025b) Nature of crime: Fraud and computer misuse – Year ending March 2024. Available at: https://www.ons.gov.uk/releases/natureofcrimetablesyearendingmarch2024.

OSR (2025) *Review of Fraud and Computer Misuse Statistics for England and Wales*. London: Office for Statistics Regulation.

Passenger A (forthcoming) Identifying telemarketing fraud victimisation through analysis of trueCall nuisance call blocking metadata – A realist evaluation of a situational crime prevention initiative. Professional Doctorate, Cardiff University.

Phillips C (2017) From 'Rogue Traders' to organized crime groups: Doorstep fraud of older adults. *The British Journal of Criminology* 57(3): 608–626.

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.

Prenzler T (2020) What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice* 6(1): 83–96.

PSR (2024) *Authorised Push Payment (APP) Scams Performance Report*. London: Payment Systems Regulator.

Public Health England and College of Policing (2019) *Public Health Approaches in Policing. A Discussion Paper*. London: Public Health England.

Scottish Government/EKOS Limited (2021) *Preventative Spend Research 2018*. Edinburgh: Scottish Government.

Shepherd J (2007) Preventing alcohol-related violence: A public health approach. *Criminal Behaviour and Mental Health* 17(4): 250–264.
Shepherd J (2023) The Cardiff model for violence prevention. Available at: https://www.cardiff.ac.uk/documents/2665796-the-cardiff-model-for-violence-prevention.
Sidebottom A and Tilley N (2023) Broadening the public health approach to policing. *Policing: A Journal of Policy and Practice* 17: paad064.
Skidmore M (2020) *Protecting People's Pensions: Understanding and Preventing Scams*. London: Police Foundation.
Southworth R (2013) *Financial Crime Control: Risk, Regulation and the Role(s) of the UK Banking Sector*. PhD thesis. Cardiff: Cardiff University.
Sparrow M (2008) *The Character of Harms: Operational Challenges in Control*. Cambridge: Cambridge University Press.
Tilley N (2024) *Better Crime Prevention*, 2nd ed. London: Routledge.
UK Finance (2024) *Annual Fraud Report 2024*. London: UK Finance.
van der Wagen W, Fischer T, Matthijsse S, et al. (2021) Unique Offender, Unique Response? Assessing the Suitability and Effectiveness of Interventions for Cyber Offenders. In: Weulen Kranenbarg M and Leukfeldt R (eds) *Cybercrime in Context. Crime and Justice in Digital Society*. vol. 1. Cham: Springer.
Victim Support (2022) Empowering those affected by crime: 2021–22 annual report and accounts. Available at: https://www.victimsupport.org.uk/wp-content/uploads/2022/11/Annual_Report_and_Accounts_2021-2022.pdf.
Wall DS (2024) *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. Cambridge: Polity.
Whitty M (2018) 419-It's just a game: Pathways to cyber-fraud criminality emanating from West Africa. *International Journal of Cyber Criminology* 12(1): 97–114.
Williams M (2016) Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology* 56(1): 21–48.