



# Practitioner perspectives on what works in preventing fraud against older adults

Mark Button<sup>a,\*</sup>, Vasileios Karagiannopoulos<sup>a</sup>, David Shepherd<sup>a</sup>, Annie Kirby<sup>a</sup>,  
Julak Lee<sup>b</sup>, Joon Bae Suh<sup>c</sup>, Jeyong Jung<sup>d</sup>, Chol Soo Koh<sup>e</sup>

<sup>a</sup> Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth, UK

<sup>b</sup> Chung-An University, Seoul, South Korea

<sup>c</sup> Korean National Police University, Assan, South Korea

<sup>d</sup> Department of Police Administration, Soonchunhyang University, Asan-si, South Korea

<sup>e</sup> Korean Financial Crime Prevention Association, South Korea

## ARTICLE INFO

### Key words:

Fraud  
Prevention  
Older adults  
What works

## ABSTRACT

Fraud is one of the most common crimes experienced by older adults in the UK and compared to younger generations, has disproportionate impact. It is becoming an increasingly critical public policy issue. However, there has been very little research evaluating what works in fraud prevention. This paper provides a unique insight into what works in preventing scams against the elderly population. Using both interviews (n = 17) and a survey (n = 334) to collect the perceptions of experts, the research rates the effectiveness of prevention methods organised into a taxonomy of four strategic themes: digital technology interventions, education, third-party control, and partnerships. Based on the experts' perceptions, the most effective methods are digital technologies that block scam communications, interventions by trained bank and care professionals, high specificity education, and coordinated partnerships to deliver prevention strategies. As well as actionable insights, the paper offers recommendations for further research.

## 1. Introduction

Fraud has become the most common crime against individuals in the UK, accounting for nearly 40% of all crime (ONS, 2023). Most of these frauds are scams perpetrated online with an international dimension and using a wide range of methods, which makes the police response very challenging (Cross, 2020; Home Office, 2023; Lazarus, 2024; Lazarus et al., 2023). In this context, the most effective solution to tackle the problem of fraud is prevention. However, compared to traditional crimes there is a lack of awareness of what tools exist to prevent fraud and, importantly, even less evidence of what actually works (Button et al., 2023b; Prenzler, 2020; Sherman et al., 1998). Indeed, there is very little high-quality research on what works in combatting fraud generally. To illustrate this, consider the respected Arizona State University (ASU) (n.d.) database of studies on situational crime prevention that work based upon the highest quality evaluation methodologies. For fraud there are only seven studies in total listed: three of which cover plastic card fraud and cheque forgery, one related to welfare fraud, two on commercial fraud against retailers and one on phonebooth fraud –

with none related to scams in general or against older adults. Juxtapose that to burglary where 46 studies were listed (ASU Center for Problem Oriented Policing, n.d.). This illustrates the clear gap in research on what works in preventing fraud.

Although older adults are often perceived as more vulnerable to fraud (Burnes et al., 2017), they have historically been the least victimised age group in the UK (ONS, 2020). However, recent data indicates that victimisation rates in the over 65 y group is increasing, driven in part by an increasing level of online engagement (ONS, 2021, 2023). Furthermore, older adults often suffer much greater financial and emotional impacts (Burnes et al., 2017; Button et al., 2024b; 2025). Preventing fraud against older adults is therefore an increasingly important issue for public policy, the police and the wider prevention community. Some research has been conducted to identify prevention methods (for example, Wilson et al., 2024), but there is little evidence that they are effective (Button et al., 2024c).

Ideally there would be a significant stream of funding to evaluate what works in preventing fraud such that this paper would be presenting findings from an evaluation rooted in rigorous scientific methodologies

\* Corresponding author.

E-mail address: [mark.button@port.ac.uk](mailto:mark.button@port.ac.uk) (M. Button).

<https://doi.org/10.1016/j.jeconc.2026.100213>

Received 6 November 2025; Received in revised form 3 March 2026; Accepted 4 March 2026

Available online 22 March 2026

2949-7914/© 2026 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

that use randomised control experiments. Sadly, such funding and research does not exist at present. Practitioners still need leads on what might work to best prioritise their resources. In the absence of such evidence this paper uses lesser quality evidence to provide some insights on what works. It provides evidence of the most effective methods to prevent scams against older adults based upon the perceptions of professionals who deal with this problem. Building upon the work of Button et al. (2024c), who mapped methods commonly used to prevent fraud against older adults, the present study used a survey and interviews with professionals to generate evidence on what they considered the most effective prevention methods. The methodological design is not at the standard of a Maryland/Sherman intervention evaluation (Sherman et al., 1998); nevertheless, it provides important insights for professionals and policymakers with responsibility for preventing fraud on what best to do. The central research question of this study can therefore be identified as:

- In absence of high-quality evidence of what works in preventing fraud against older adults what can we learn from experts and their experience in tackling these problems in what they believe is most effective?

This paper begins with a brief review of the scholarship relating to fraud victimisation and prevention. It subsequently describes the research methods, introduces the findings organised into a taxonomical framework and then discusses the implications with some actionable insights and recommendations for further research.

## 2. Fraud, older adults and prevention

Frauds against older adults have become a significant problem in many jurisdictions (Cross, 2021; DeLiema et al., 2020a; Global Anti-Scam Alliance, 2025; Kemp and Erades Pérez, 2023; Kim et al., 2025). England and Wales are one of the few countries that conducts a regular largescale victimisation study that includes questions on fraud. In recent years, older adults in England and Wales have become more likely to become victims of fraud. Fig. 1 reproduces the fraud victimisation rates across a range of age categories from 2019 to 2023 from the Crime Survey of England and Wales (ONS, 2023). Victimisation rates increased across all age categories during the pandemic but, excluding that period, have remained relatively stable except for the older age group (65 y and over), where the rates have increased to about 5%.

Compared to younger generations, fraud tends to have a greater impact on older adults (Button et al., 2025). Button et al. (2024c) found that the average loss to a fraud in the 18–24 y age group (£2052) is a fraction of the losses in the 65–74 y (£10,231) and 75 y + (£13,112) age groups. Fraud can also cause fear, lead to physical and mental health problems, change behaviours negatively and even lead to suicide (Bailey

et al., 2021; Button et al., 2014, 2021, 2024a and b; 2025; Cross, 2016; Deliema et al., 2020a and b). Preventing fraud against the older age group is, therefore, an increasingly critical public policy issue.

There have been only a few studies that have explored the effectiveness of methods that prevent fraud against organisations and individuals, and they typically bemoan the lack of quality evidence (Button et al., 2023; Prenzler, 2020). The few studies offering some evidence in support of effectiveness focus on specific prevention methods; they can be organised into three categories: education, technology tools, and third-party intervention.

### 2.1. Education

A range of studies have been conducted into strengthening the resilience of individuals to scams by raising awareness and self-protection through educational campaigns and training. Several experimental studies suggest that educational methods do reduce individuals' susceptibility to scams (AARP, 2003; Burke et al., 2022; DeLiema et al., 2025; Kubilay et al., 2023; Scheibe et al., 2014). Whilst the experimental and statistical nature of these studies is persuasive, they are based on artificial conditions using a specific type of mock scam, very short videos or interactive training, or very brief scam warnings. Consequently, the extent to which the results reflect the real world is questionable. Indeed, experimental findings conflict with the results of real-world research. With access to real-world data in a Danish bank, Jensen et al. (2024) found that brief scam warnings had no effect on victimisation. Similarly, Smith and Akman (2008) monitored the results of an anti-scam campaign in Australia and New Zealand and found that it failed to impact on victimisation rate.

Button et al. (2024a) pursued a different approach, giving voice specifically to older persons through interviews and a survey to give their views on what works for them. They found that, although some older adults become more aware of scams and prevention techniques through multi-media campaigns, the best way to educate and support them is through family, friends or trusted others. The study did not empirically investigate the impact of education.

### 2.2. Technology tools

The limited literature on the use of technology to detect scams primarily focuses on technical efficacy. For example, Hong et al. (2023) and Derakhshan et al. (2021) propose machine learning techniques that detect scam calls with between 85% and 93% accuracy. One study examined the real-world impact of a proprietary product for blocking spam calls and landlines, trueCall Secure,<sup>1</sup> which is specifically designed for older adults (Rosenorn-Lanng and Corbin-Clarke, 2020). They found that the percentage of users who received at least one scam or nuisance call over a six month period fell from 94% to 8%.

### 2.3. Third-party intervention

Studies have shown that third-party interventions can be successful in disrupting scams by either warning people that they are victims of ongoing scams or by preventing scams at the moment of transaction. Mills et al. (2012) ran a small field trial with healthcare professionals in the US. Following the provision of vulnerability training, 24 out of 35 professionals reported the identification of 25 patients they felt were vulnerable to elder financial abuse. Although this trial is too small to be convincing and it had no impact on crime reduction, it does point to the merits of social interventions.

A far more convincing study drew on data from Operation Sunbird in Australia. The police operation used financial intelligence to disrupt ongoing transnational scams. It focused on money transfers to West

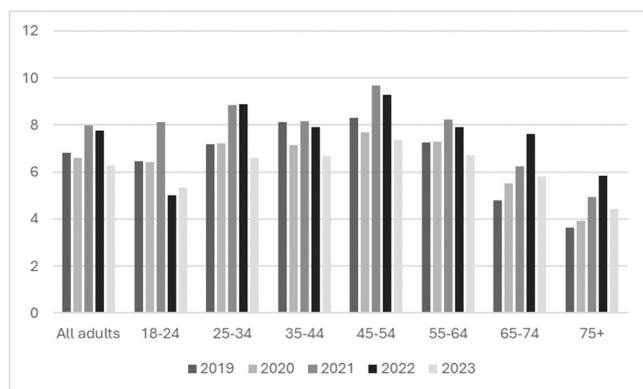


Fig. 1. Percentage of age groups victims of fraud. Note: data from ONS (2023).

<sup>1</sup> trueCall Secure <https://www.truecall.co.uk/category-s/117.htm>

Africa, identified suspicious completed bank transactions and contacted the account holders to warn them that they were likely victims of advance fee or romance fraud; 82% subsequently stopped transferring money (Cross, 2016). The BankSafe programme run by the AARP Public Policy Institute in the US protects elderly people by focusing the locus of control at the moment of transaction.<sup>2</sup> The programme trains bank staff to spot signs of elder financial abuse and actively intervene. A large field study conducted with financial institutions in 2018 measured the impact: fraud detection increased fivefold, and the money saved increased by a factor of 16 (AARP, 2019).

Beyond this limited scholarship, there is very little robust evidence to guide the selection of methods, strategies or public policy for protecting older adults against the scam threat. The purpose of the present study is twofold. Firstly, based on the collective perceptions of experts, it aims to provide evidence of the effectiveness of a range of methods for preventing fraud against elderly persons organised into a taxonomical framework. Secondly, it provides an agenda for prioritising further research and robust testing.

3. Methods

The growing problem of scams in general and in-particular against older adults requires action, but there is not an evidence-base of high-quality evaluation to guide such responses. In the absence of that a useful strategy is to seek the opinions of those that use different tools and strategies. They will at least have a feel of what might be impacting on the problem they are dealing with. It is a quick and alternative means to gather evidence on what might work, which can be used not just by practitioners but also future researchers in prioritising high-quality evaluations. We do not claim the results of this research are equivalent to Maryland ranked studies, but the evidence offered is better than no evidence. There are clear limitations to such approaches as illustrated by Tetlock and Gardner (2016) who exposed political experts’ ineffectiveness in predicting the future – something we must note is different from reflecting on something they have experience of using and whether it has an impact.

The research strategy is therefore based on experts’ perceptions of effectiveness as opposed to directly measuring the causal impact of interventions. Whilst experimental methods using fabricated conditions yield statistically sound results, they have to be viewed with caution (for example, Burke et al., 2022; DeLiema et al., 2025; Kubilay et al., 2023; Scheibe et al., 2014). Large field studies are robust but require significant resourcing and collaboration. Furthermore, both of these approaches are inevitably limited with respect to the range of scam types and prevention methods that they can practically accommodate, typically one type and one method.

In contrast, an analysis of perception allows the inclusion of a broad range of prevention methods. This aids the consideration of broader strategies and public policy in the short term. It also helps inform the selection of methods for targeted further testing, ideally by real-world field trials. The research strategy involved three data collection elements. First, a literature review of both academic and other sources was undertaken to identify a broad range of methods used to prevent fraud against older adults. The identified methods informed the subsequent data collection phase, which was completed during 2022–24.

Second, 17 interviews were conducted with professionals working in the police, government bodies, NGOs and companies offering prevention services (Appendix A). The majority (15) of the interviewees were based in the UK with one from the USA and another from South Korea. The interviews were mostly conducted via Zoom, recorded and transcribed. They provided a rich insight into the participants’ views of the prevention methods.

To provide a quantitative insight into effectiveness, the third element

was a survey of 334 professionals working in this field (Appendix B). The survey invitations were distributed through the authors’ extensive professional networks on LinkedIn, the contact list of the [anonymised], which contains over 3000 individuals working in counter fraud, and to key individuals for distribution within their own networks. The largest group of respondents were local government Trading Standards Officers, accounting for 18% of the sample. Employees of the national government and the police were also well represented. The UK is over-represented at 75% of the sample. A quarter of the respondents were spread across 21 nations: Australia, Belgium, Bulgaria, Canada, Estonia, Germany, Hungary, Italy, Lithuania, Malta, Nigeria, Netherlands, Norway, Poland, Seychelles, Singapore, South Korea, Spain, UAE, USA and Venezuela.

The nature of the sample framework means there are limitations to the generalisability of the findings. It is nevertheless a substantial sample of experts offering important views on what works in preventing fraud against older adults. The research achieved ethical approval from [anonymised] (number #) prior to commencement and all participants provided their consent to participate.

4. Findings

The research of Button et al. (2024c) identified dozens of different strategies and products which are used to prevent frauds against older adults. To provide more coherence to this they divided them into the following key areas: traditional crime prevention, such as physical products like spyholes, awareness campaigns etc; crime prevention rooted in modern technology, such as call-blockers; crime prevention rooted in technologies associated with the Fourth Industrial Revolution such as apps using artificial intelligence etc; and partnerships. To make these distinct groups more manageable for this research the research findings are organised taxonomically into six strategic groups drawn from the taxonomy above: 1. physical methods, 2. disrupting communication, 3. education programmes, 4. personal prevention, 5. third-party controls, and 6. the police and criminal justice system. The questionnaire asked respondents to rate a wide range of prevention methods on a scale of 1–5, where (1) is not very effective, (2) is ineffective, (3) is neutral, (4) is effective and (5) is very effective. The results were subsequently collapsed into two categories: effective (effective or very effective) and ineffective/neutral (not very effective, ineffective or neutral). The analysis of effectiveness is therefore based on the collective view of the respondents, the proportion who perceive each method as effective (Tables 4–8).

4.1. Physical methods

Physical measures are frequently advocated for defending against in-person doorstep scams and rogue traders (Neighbourhood Watch, n.d.). Table 1 sets out the respondents’ views of the effectiveness of five methods. Of these, only video doorbells rate highly, scoring 75%. The collective view of the other four methods is that they are much less effective. This is also reflected in the interviews.

“Stickers and things like that, I know to be frank, if they’re prepared to go and scam somebody at the door, I’m not sure what a, you know,

Table 1  
Physical methods.

| Physical method               | % effective |
|-------------------------------|-------------|
| Video doorbells               | 75%         |
| Postal block                  | 54%         |
| Personal alarms               | 40%         |
| Spyholes                      | 38%         |
| No cold caller stickers/signs | 27%         |

<sup>2</sup> AARP BankSafe <https://www.aarp.org/pri/initiatives/banksafe/>

cold caller... That will dissuade the honest person as a cold caller, but it won't dissuade a scammer." (Ted, Police Officer)

#### 4.2. Disrupting communication

The survey respondents were presented with a variety of technology tools to disrupt communications and transactions between fraudsters and victims. Most of the methods are rated highly at 70% and above (Table 2): real-time transaction alerts, such as text warnings from banks about suspicious transactions or alerts immediately prior to executing a transaction, spam detection, telephone call blockers, call warning apps that signal suspected scams and spam, and anti-virus tools.

Although prior research into call blockers has been positive (Rosenorn-Lanng and Corbin-Clarke, 2020) and these tools were rated high in our survey, the views of the interviewees were mixed.

"I'm not entirely sure that they (call blockers) continue to be as effective. And they're all landline based, so, you know, a lot of this is now mobile phone based. .... So, I'm just not sure that's going in the right direction." (Ted, Police Officer)

It seems that Ted is unaware that call blockers are available for mobile phones, which suggests that some experts are not keeping abreast of emerging technologies. An NGO worker noted the mental health benefits to many older adults of reducing the number of nuisance calls, but was unsure about the effectiveness of call blockers in preventing scams.

"But I think that has been quite effective from...particularly from a kind of like mental health perspective for some of those clients who are receiving a lot of nuisance calls. But obviously, we can't say for sure whether they prevented a fraud but it would indicate that that is the case as well." (Kirstie, NGO)

In contrast, Dickie (US NGO) and Kim (South Korean police) felt that technology apps such as Nomorobo<sup>3</sup> and Konan Citizen<sup>4</sup> are effective. Nomorobo is a mobile app that blocks spam calls and texts. Konan Citizen is similar to anti-malware software with a broader range of functions: it automatically detects and disrupts malware and malicious activity, intervenes in scam calls and blocks transactions. The implication is that the effectiveness of technology solutions depends on their specific application, landline or mobile telephones, and the breadth of their functionality: mobile apps with an integrated suite of defensive functions are likely to be more effective than those, such as call-blockers, that perform a single task.

#### 4.3. Education programmes

Fraud awareness and prevention education programmes are common strategies. However, most of these methods were not highly regarded in the survey (Table 3). The best methods involve specificity: targeted fraud alerts designed for specific age group (77%), targeted awareness

**Table 2**  
Technology tools for disrupting communication.

| Technology method       | % effective |
|-------------------------|-------------|
| Transaction alerts      | 78%         |
| Spam detection          | 75%         |
| Telephone call blockers | 74%         |
| Call warning app        | 70%         |
| Anti-virus              | 70%         |
| Caller identification   | 55%         |
| Malicious app tool      | 53%         |

**Table 3**

Effectiveness of fraud awareness and prevention education programmes.

| Method                                                  | % effective |
|---------------------------------------------------------|-------------|
| Targeted fraud alerts – designed for older adults       | 77%         |
| Targeted awareness campaigns – highlight specific scams | 77%         |
| One-to-one training                                     | 73%         |
| Scam training (group)                                   | 67%         |
| Presentations                                           | 63%         |
| Cyber-training                                          | 63%         |
| General awareness campaigns                             | 57%         |
| Broadcast fraud alerts – general                        | 53%         |
| Scam awareness tests + advice                           | 46%         |
| Leaflets                                                | 38%         |
| Phishing awareness tests + advice                       | 37%         |
| Websites (general information and advice)               | 25%         |

campaigns that specifically highlight an emerging scam type, and very specific one-to-one training (73%). Broader educational programmes, such as group training, presentations, general awareness and leaflets were not well-regarded.

The experts are also clearly sceptical about the value of scams and phishing awareness testing. Similar to penetration tests, individuals' responses to fake attacks are tested and advice is given to those who fail. These methods are controversial with several participants from the UK actually opposing them on ethical grounds:

"It's not something we have ever done and I'm not sure it would really sit with my values." (Ted, Police Officer)

"I don't like it because I think it makes people feel stupid. It's been used before .... and I think that perpetuates the blame and the shame, and the effects of it." (Laura, Trading Standards Officer)

The main implication of the survey results is that the specificity of educational programmes is an important consideration. This finding is supported by the interview data. Anne noted the need to use multiple channels to access older adults with specific messages.

"Awareness, awareness, all the time, in every opportunity we get. Other than the bulletins that go out, it's a case of whenever we have some success with something, whatever it is, or there's awareness messages that need to go through the media, the local media, whoever it is, getting out through social media, as well as through the press, awareness is the main thing. .... We have no doubt that we are preventing a lot of crime within the [name] area." (Anne, NGO).

Another NGO worker, Dave, uses the specificity of a road safety metaphor to convey a safety message whilst neutralising fears that may cause older people to withdraw from social interaction.

"I liken it to road safety. So, I often say this in awareness sessions, because you can see the fear coming up. But actually, cars are a lethal weapon ... we can still be severely hurt or killed by a car, and yet we still go out and about because cars are part of our daily life. However, we were taught from an early age something that would help prevent those accidents by looking left, looking right, looking left again, kind of thing. So, I think if we can get over to them that scams aren't going away, just like cars aren't. But therefore, we can just learn simple steps to protect ourselves and still be able to go about our daily lives and include technology and socialisation and stuff as well." (Dave, NGO)

The operation of Dickie's NGO illustrates the importance of linking broader educational campaigns to the specificity of one-to-one support via hotlines, similar to the Samaritans.

"We have over 20,000 of them [volunteers]. ... They go out and they give speeches. We have a call centre in [name of city] .... now everybody knows about it because we've promoted the hell out of it and so they get 2000 calls a week from just people who are...you know, it's another hotline basically." (Dave, US NGO)

<sup>3</sup> Nomorobo <https://www.nomorobo.com/>

<sup>4</sup> Konan Citizen <https://konan-citizen.en.uptodown.com/android>

Jack and Laura also noted the value of engaging with local communities. This approach enables them to then reach individuals for one-to-one engagement and advice. Importantly, it also stimulates peer-to-peer support within the community.

“I found one of the most effective ways to protect vulnerable elderly people from becoming a victim was to speak to them in person. In 2016/17 I conducted dozens of presentations at community halls, sheltered accommodation, church halls, parish halls, etc. This allowed them to engage with a ‘real’ person and ask questions which is vital. They shared their experiences, some of whom admitted having been a victim but too embarrassed to say/report. I was able to address each of their issues.” (Jack, Police Officer)

“... it gives almost that permission for people to start talking about their own experiences. And peer-to-peer support in a fraud and scams perspective is one of the most valuable things that we can do.” (Laura, Trading Standards)

#### 4.4. Personal prevention

The personal prevention methods were not generally well-regarded in the survey (Table 4). Websites like <https://www.scamadviser.com/> enable a person to assess how risky a website is for potential fraud were rated as effective by just 61%. Services for checking one’s own personal information, for example <https://haveibeenpwned.com/>, were rated even lower at 52%. Helplines, scam registers, where known scam companies are listed on websites, and trusted trader schemes were viewed by around half as effective Tables 4–8.

#### 4.5. Third-party controls

The most highly rated methods are highly specific and interventionist third-party controls (Table 5). At the top of the list, and the highest rated (91%) of all the methods in the study, is intervention by trained bank staff when they spot the signs of an active fraud against a customer (see AARP, 2019). Similarly, the respondents regarded community-based interventions by trained care professionals as effective (87%): for example, doctors, social workers and care workers (see Mills et al., 2012).

Data analytics (86%) and protective flags on bank accounts (84%) continue the specific interventionism and community care themes. Data analytics use algorithms to detect suspect transactions and prompt automatic or human interventions that require customers to confirm transactions. Protective flags modify the detection algorithms by reducing the intervention threshold on the bank accounts of vulnerable customers. They also signal to bank staff the need for enhanced vigilance of these accounts. Protective flags are a consequence of some kind of risk assessment by the police, banks or other agencies, and may be triggered by actual victimisation.

The advanced identification tools, facial recognition and voice pattern recognition, are viewed less favourably. This may be because their utility is limited to schemes where the fraudsters try to impersonate older adults. Supervision of bank card activity, either by monitoring or sharing cards, is not viewed as effective and, paradoxically, increase the risk of fraud by a trusted family member or friend as found in the AARP (2019) study. Although social prescribing is a recognised approach

**Table 4**  
Effectiveness of personal prevention methods.

| Method                                                                                                   | % effective |
|----------------------------------------------------------------------------------------------------------|-------------|
| Website checker, e.g. <a href="https://www.scamadviser.com/">https://www.scamadviser.com/</a>            | 61%         |
| Helplines                                                                                                | 56%         |
| Personal information checker, e.g. <a href="https://haveibeenpwned.com/">https://haveibeenpwned.com/</a> | 52%         |
| Scam register (warning lists)                                                                            | 51%         |
| Trusted trader schemes                                                                                   | 49%         |

**Table 5**  
Effectiveness of third-party controls.

| Third-party controls                                     | % effective |
|----------------------------------------------------------|-------------|
| Trained bank staff intervention                          | 91%         |
| Trained care professional intervention                   | 87%         |
| Data analytics detection (e.g. by banks)                 | 86%         |
| Protective flags on bank accounts                        | 84%         |
| Facial recognition (e.g. by banks)                       | 69%         |
| Risk assessments                                         | 65%         |
| Voice pattern recognition (e.g. by banks)                | 62%         |
| Third-party bank card monitoring (e.g. by family member) | 61%         |
| Social prescribing activities                            | 46%         |
| Shared bank cards (e.g. with family member)              | 26%         |

**Table 6**  
Effectiveness of policing and criminal justice system.

| Method                                   | Overall | UK  | Overseas |
|------------------------------------------|---------|-----|----------|
| Disrupt local organised crime groups     | 62%     | 59% | 71%      |
| Disrupt overseas organised crime groups  | 57%     | 53% | 67%      |
| Police prevention activities             | 47%     | 40% | 69%      |
| Prosecution of fraudsters/cybercriminals | 45%     | 40% | 60%      |
| Police investigation                     | 43%     | 35% | 65%      |
| Sentencing of fraudsters/cybercriminals  | 37%     | 31% | 53%      |

**Table 7**  
The importance of fraud prevention partnerships.

| Type                  | Important | Not important | Don’t know |
|-----------------------|-----------|---------------|------------|
| National partnerships | 89%       | 1%            | 10%        |
| Local                 | 92%       | 1%            | 7%         |

**Table 8**  
Respondents’ awareness of fraud prevention partnerships.

| Type     | Yes | No  | No answer |
|----------|-----|-----|-----------|
| National | 35% | 63% | 1%        |
| Local    | 32% | 67% | 1%        |

(Cooper et al., 2022; Office for Health Improvement and Disparities, 2022), the professional respondents in our survey require further convincing, which suggests the need for further research and/or stronger advocacy.

#### 4.6. The police and criminal justice system

The response of the police and criminal justice system to fraud in the UK is inadequate (Button, 2021; Cross and Blackshaw, 2015; Her Majesty’s Inspectorate of Constabulary, Fire and Rescue Services [HMICFRS], 2019; Police Foundation, 2018). Therefore, it is not surprising that the survey yielded a low set of scores (Table 6). However, a major influence on these results is jurisdictional: law enforcement is the only category of prevention methods where the results of the UK and overseas respondents diverge. Compared to the UK, Table 6 shows that the overseas respondents have a substantially higher regard for the effectiveness of law enforcement in their jurisdictions across all the factors. This finding calls for further comparative research.

Nevertheless, because organised crime groups cause high volume, widespread harm, disrupting both local (overall 62%) and overseas groups (overall 57%) is viewed by both UK (59%/53%) and overseas (71%/67%) respondents as the most effective law enforcement strategies. The other traditional crime prevention and deterrence activities of the law enforcement are widely regarded as ineffective, especially sentencing policies (37%). These results are an inevitable consequence of public policy which heavily prioritises physical crime over fraud, a policy that is well-recognised in the literature and by the participants.

"So, if I got burgled in my own home or somebody mugged me, I would get victim support, I would get, potentially a visit from a police officer, I would get a phone call to check that I was okay, do I need extra support, et cetera. We don't do that for fraud and scam victims, we don't provide that aftercare, there's no enhanced victim support services." (Laura, Trading Standards)

#### 4.7. Partnerships

Partnerships are not common in fraud policing and prevention, although there are some notable examples in the UK, such as Operation Signature in Sussex, National Hunter (data sharing), and Scamwise Northern Ireland (Goldstraw-Wright et al., 2024). The respondents were asked to rank the importance of such partnerships on a scale of 1–5 where (1) is not very important, (2) is not at all important, (3) is neutral, (4) is important and (5) is very important. The results are collapsed into 'important', 'not important' and 'don't know' in Table 7.

The overwhelming majority (about 90%) of respondents view both local and national partnerships as important. Paradoxically, however, about two-thirds of the respondents are unaware of any partnerships (Table 8). It seems that the majority of the professional community intuitively like the idea of partnerships, but collaborative arrangements are not prominent in the collective battle against fraud. The interviewees, who also favour partnerships, provided some insight into this problem. They felt that partnerships are ad hoc, uncoordinated and invisible. In this sense, the landscape of partnerships mirrors the fractured landscape of law enforcement agencies that deal with fraud (Button et al., 2022). Some participants called for leadership from the government to develop a coherent strategy with clarity on the purposes of partnerships, visibility and funding.

"But I think it's more having a plan set out by the Home Office. I know they've made it kind of a priority in the new police requirements yet there's not much talk in terms of like what the actual plan is ... like they're tackling the issue when they're really not." (James, NGO)

"It's a more like structural issues that seem like they need to be resolved. And like the actual kind of way that things are funded, you know, the strategies that sit behind them, like where people should go for what, that kind of stuff, it just doesn't feel very clear." (Kirstie, NGO).

#### 4.8. Methods suggested by participants

Reflecting on their frustrations, some of the interview and survey participants were keen to promote additional strategies and tactics. Similar to Button et al. (2023a), several pointed to the culpability of technology companies in facilitating scams.

"The internet is the main vector of fraud, so the internet has to be the answer... I am working with tech companies, but ... they're not doing the bare minimum at the minute. I think we have to incentivise companies to do more. (Louise, civil servant)

"A greater level of proactivity from telecommunication and social media companies to stop phoney websites/emails and to scammers purchasing phone numbers which they can then use to phone older people on." (Respondent 26)

Social media platforms taking more responsibility (Respondent 83).

Facebook and other social media to improve their response to reports of scams and cloned accounts. It's far too easy for a scammer to clone a Facebook account and scam vulnerable people out of money believing they are responding to a request from a "friend" (Respondent 106).

Some respondents suggested reversing the race to high-speed bank transactions, creating greater friction in payments with a cooling-off period before funds are actually released or a staggered release.

"With on-line banking, when a payment is made it is marked 'pending' for 24 h to allow a recall of the funds." (Respondent 67)

"Recipient verification, staggered release of funds to new recipients." (Respondent 106)

Survey respondent 150 suggested a service older people could go to for advice (see Karagiannopoulos et al., 2021).

"It would be good if older adults had someone they could go to for advice - maybe scam experts in banks/befriending services (in case the older adult is unable to get out of the house much) who are available for them to bring their mail/talk about emails/calls they've received to ask advice - it might help to break the stigma a bit because it's not as formal as having to phone to report, it's an open door for anyone to ask." (Respondent 150)

## 5. Discussion

This discussion focuses on the strategic themes and methods the research participants believe are the most promising in protecting elderly persons: education, partnerships, disrupting communication, and third-party controls.

### 5.1. Education

The educational awareness campaign is the most obvious public-facing strategy. It is also the most obvious response when a demographic group is perceived to be particularly vulnerable and lacking self-protection skills. However, the collective view of the practitioners in our study concurs with previous research that it is important to design specificity into the design of educational programmes. Widely broadcast campaigns that target the general population are low specificity and, as Smith and Akman (2008) showed, they are unlikely to bear down on victimisation rates. The practitioners believe, like Karagiannopoulos et al. (2021) and Button et al. (2024a), that high specificity education is more effective, that is, by targeting specific groups or even specific individuals in a one-to-one setting. Such education is most effective when delivered by trusted others, e.g. family, friends, the police or NGOs, in local community settings or in the home (Button et al., 2024a).

Nudging people with shared public alerts or forewarnings about specific scams is a form of education. Our results indicate that experts are in favour of this approach, and experimental research has found that warnings by way of alerts or snappy educational videos are effective (Burke et al., 2022; Scheibe et al., 2014). However, real-world research by Jensen et al. (2024) found that this method does not reduce victimisation rates. The explanation for these divergent results may be contextual. The experiments cognitively stimulated participants into a defensive security attitude before the specific test was executed. On the other hand, the bank clients in the Jensen study may have been focused on executing their real-world transactions and, therefore, their defensive security attitudes were not sufficiently stimulated to absorb the attack alerts. Indeed, even within the longitudinal experiments, participants' defensive awareness was found to be perishable (DeLiema et al., 2025). By this reasoning, the challenge for the nudging approach is to first stimulate a security attitude when announcing a scam warning. These considerations call for further research.

### 5.2. Partnerships

Partnership arrangements, such as police engagement with local community groups, provide routes for both stimulating defensive attitudes and follow on alerts. However, a significant problem is that most

practitioners are unaware of partnerships, the kind of services or activities they provide and whether they are appropriate for elderly persons. The partnership centred on The Cyber Helpline,<sup>5</sup> for example, is active in supporting victims of any type of cybercrime and directing them to collaborating expert volunteers for advice; it is an after-the-event service in response to attacks and access is via a chatbot, which may not be appropriate for everyone. In contrast, LoveSaid<sup>6</sup> is an advocacy organisation that focuses on romance fraud. It publishes advice and collaborates with law enforcement, academia, and other NGOs in developing awareness, guides and so on, but it does not directly engage with victims; its purpose is more concerned with developing awareness and practices for tackling the problem.

These kinds of collaborative arrangements are valuable. However, because they have emerged organically to focus on specific problems or services, the practitioners sense the absence of a coherent strategic direction. They called for government leadership in supporting partnerships and, importantly, making them far more visible. Invisibility is bound to compromise their impacts, and, if experts are unaware of them, it is reasonable to assume that the bulk of the public are unaware too.

### 5.3. Disrupting communication with technology

Breaking the link in communication between the scammers and older adults is important: real-time transaction alerts, spam and scam warnings, call blockers and anti-virus tools are regarded as effective defences. Despite some reservations amongst the interview participants, research has demonstrated the efficacy of call blockers on landlines (Rosenorn-Lanng and Corbin-Clarke, 2020). The obvious advantages of automated blocking technology is that it is direct, immediate and, crucially, the user is not required to deliberate on the legitimacy of the communication.

However, two problems are emerging. Firstly, the rapid development of applications with an integrated range of defensive functions, including transaction blockers, appears to be leaving some experts behind, so it is reasonable to assume that many citizens are even less aware. Moreover, this awareness gap may be exacerbated by the accelerated development of automated and artificial intelligence tools (Bajaj and Edwards, 2023; Chouhan et al., 2024; Edwards et al., 2017). These problems could be addressed with a coordinated network of partnerships to disseminate and advertise new technology tools. Secondly, the effectiveness of the latest applications is unknown. This is where a partnership involving consumer organisations such as Which?<sup>7</sup> and the City of London Police could be incentivised to set up a rolling programme of evaluations similar to the Rosenorn-Lanng and Corbin-Clarke (2020) study.

### 5.4. Third-party controls

The most highly rated prevention methods are third-party controls that detect the signals of fraud victimisation and prompt intervention. All the methods in this group are high specificity and interventionist in directly preventing fraud threats to specific individuals. The highest rated method is the immediate intervention in transactions by bank staff who have been trained to spot the signs of victimisation (see also AARP, 2019). This 'in-the-moment' institutional approach is supported by the use of data analytics to identify risky transactions and behaviours, and protective flags on customer accounts. These analytical outputs furnish bank staff with intelligence to assist in appraising the vulnerability of customers when transactions are attempted. As well as the in-the-moment interventions, data analytics has the capacity to trigger interventions by identifying vulnerability to ongoing scam schemes

(Cross, 2016).

The second highest rated is intervention by trained care professionals, who are more likely to have personal knowledge of elderly persons. The professionals may be present to provide in-the-moment interventions, but their defensive contribution is more likely to be in identifying vulnerability or signs of ongoing scams, raising concerns with the individual, and calling on appropriate support. A notable feature of these highly rated controls is that they are exercised by independent actors outside the family circle. In contrast, intervention controls that would typically be exercised by family members, third-party monitoring of bank card use and shared bank cards, are viewed much less favourably. A significant problem with these family-based controls is the displacement of fraud risk from a remote scammer to a close but dishonest relative. The AARP (2019) field trial found that in 70% of detected cases of elder financial abuse, the fraudsters were family members.

### 5.5. Digital defences and social control

Our research focused the fraud prevention question on older adults, but the results are also relevant to younger people, who are more likely to be fraud victims (ONS, 2023). The challenge is succinctly summed up by one of the participants:

"So, I think it's some version of... forewarned is forearmed but more importantly, hardening the target, building a sort of informational moat around the person.... It's hardening the target idea. You know, it's becoming so difficult even for fully cognitively sound human beings like you and I to figure out what's real and what isn't real." (Dave, US NGO)

Similarly, drawing on an engineering metaphor, Button et al. (2023a) illustrated the huge scale of the threat forces in favour of fraud to argue that it is not feasible to expect an individual of any age to have the capacity to continuously and reliably resist these forces. They also argued that, in the context of the global reach of high volume scam schemes, it is impossible for the police to arrest the problem away. They called for a rearrangement of the forces so as to better protect the individual, for example by shifting internet service providers, social media, telecoms firms and banks from efficient facilitators of fraud to defenders against fraud. The study's practitioners are clearly of a similar mind: law enforcement is ineffective so that protection rests on digital and social controls.

Four strategic themes emerge from the analysis, all of which contribute to building layers of safeguarding forces around older adults with digital defences and effective social controls. Firstly, the collective view of the practitioners is that digital technical solutions which block the receipt of scam communications are effective, though social media companies, especially Facebook, need to move beyond the pretence of corporate window dressing to a values orientated (Weaver et al., 1999) and socially responsible security mentality. Secondly, the high specificity educational approach in small groups or with individuals is the most obvious form of socially orientated control. Thirdly, the in-the-moment controls exercised by banks shift the relationship between the institution and the customer from a purely transactional interaction towards a more socially orientated relationship, somewhat reminiscent of client relationships before the advent of internet banking. Similarly, the practitioners support the expansion of care professionals' roles beyond the immediate care provision, again reminiscent of earlier times. But their views are not based on nostalgia, they are objectively practical social solutions.

Fourthly, delivering the prevention themes requires the collective action of capable stakeholders. Partnerships programmes should be the ideal delivery vehicles provided they are constituted with the appropriate combination of relevant stakeholders. For example, technology firms, civil society organisations and the City of London Police could collaborate in developing more effective scam blocking solutions, and

<sup>5</sup> The Cyber Helpline <https://www.thecyberhelpline.com/>

<sup>6</sup> LoveSaid <https://lovesaid.org/>

<sup>7</sup> Which? <https://www.which.co.uk/>

then deliver public education, awareness and access to the products. Banks could collaborate with NGOs to develop and deliver schemes for identifying and intervening in ongoing scams (see Cross, 2016). The problem in the UK is that the landscape of partnerships is currently fractured, lacks central coordination and is largely invisible. A government agency, such as the Home Office or the City of London Police, is best placed to provide leadership and coordination.

### 5.6. Further research

The main limitation of this research is that it is based on perceptions rather than evidence of real-world interventions. Nevertheless, it provides a valuable insight into the collective views of practitioners and an agenda for further research. Considering the explicated limitations of experimental research using artificial conditions, future research should be ambitious in using natural intervention experiments to the standard of the Maryland scale (Sherman et al., 1998). The paradoxical views of partnerships invite investigation into their utility, organisation and co-ordination. An intriguing but unexplored result, the low regard for the UK's police and justice law enforcement compared to overseas jurisdictions, calls for further research.

### 5.7. Towards an evidence-base

Traditional crime prevention has spawned a deep literature base of what works. There are hundreds of papers rooted in the highest methodologies of evaluation, dozens of systematic literature reviews analysing these works and multiple websites and databases where such evidence can be easily found. A practitioner seeking solutions to burglary is blessed with much research to make decisions on what to do to tackle it. Frauds and scams have rapidly become one of the most prominent crime problems in many countries, but as this article has illustrated there is little research based on robust scientific methods to guide policy-makers and practitioners on what to do. This article highlights some insights on what might work using a lower quality of evidence. But what this article also builds towards and illustrates is the need for a much deeper evidence-base of what works in tackling frauds and scams and sources of this evidence which can be easily found. There is a huge gap and it is hoped this article not just provides insights on what to do in the absence of this evidence-base, but also stimulates more research and initiatives to showcase that knowledge.

## 6. Conclusion

There is a profound lack of rigorous, quantitative research into what works in preventing fraud against older adults. In the absence of such high-quality evidence, this paper provides important insights into the methods that fraud prevention practitioners and policymakers should consider in developing strategies that strengthen protection for older adults. Using both interviews and a survey to collect the perceptions of

experts, the research provides a taxonomy of prevention methods rated for effectiveness. The most highly rated methods are third-party interventions by bank staff and care professionals. Technology methods, such as call blockers, that break the communications between scammers and potential victims are also highly rated. Education is considered effective when it is high specificity, that is, specifically designed for elderly persons and delivered to small groups or individuals. The findings provide a taxonomical agenda for further research, especially real-world intervention trials in the field. The cost of conducting such research is high, but the cost of not finding out what works in preventing fraud against the elderly is far higher. It is important to reiterate again the nature of this study does not provide the highest quality evidence. Just because a practitioner considers one strategy works more than another does not mean it does. Only high-quality evaluations using randomised control trials can answer that question. However, in the absence of such research the authors consider this study offers some insights which are better than none. The growing problem of frauds and scams requires action and its vital that is shaped by at least some evidence, rather than just guessing what might work.

### CRedit authorship contribution statement

**Julak Lee:** Writing – review & editing, Methodology, Funding acquisition. **Annie Kirby:** Writing – review & editing, Project administration, Methodology. **David Shepherd:** Writing – review & editing, Formal analysis. **Vasileios Karagiannopoulos:** Writing – review & editing, Investigation, Funding acquisition. **Mark Button:** Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Chol Soo Koh:** Writing – review & editing. **Jeyong Jung:** Writing – review & editing, Formal analysis. **Joon Bae Suh:** Writing – review & editing, Methodology, Investigation, Funding acquisition.

### Funding

This research was funded by the ESRC Grant number ES/W011085/1.

### Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Mark Button reports financial support was provided by UK Research and Innovation Economic and Social Research Council. Mark Button reports a relationship with UK Research and Innovation Economic and Social Research Council that includes: funding grants. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Appendix A. - Interviewees

| UK Based                            | Overseas                          |
|-------------------------------------|-----------------------------------|
| Senior police officer (Ted)         | USA NGO (Dickie)                  |
| Trading standards officer 1 (Laura) | South Korean police officer (Kim) |
| Senior civil servant (Louise)       |                                   |
| Trading standards officer 2 (Andy)  |                                   |
| Trading standards officer 3 (Bill)  |                                   |
| NGO (Anne)                          |                                   |
| Trading standards officer 4 (John)  |                                   |
| Trading standards officer 5 (Blair) |                                   |
| NGO (Dave)                          |                                   |
| NGO (Kirstie)                       |                                   |

(continued on next page)

(continued)

| UK Based                 | Overseas |
|--------------------------|----------|
| NGO (James)              |          |
| Telecom company (Hannah) |          |
| FinTech company (Don)    |          |
| Police officer 1 (Peter) |          |
| Police officer 2 (Jack)  |          |

Appendix B. - Role of survey respondents

| Role                                                             | No  | %    |
|------------------------------------------------------------------|-----|------|
| Employee of bank/financial institution                           | 28  | 8%   |
| Employee of charity/NGO                                          | 23  | 7%   |
| Employee of local government                                     | 29  | 9%   |
| Employee of national government                                  | 42  | 13%  |
| Employee of company developing/selling fraud prevention products | 23  | 7%   |
| Employee of the police service (staff or officer)                | 39  | 12%  |
| Local government Trading Standards Officer                       | 60  | 18%  |
| Voluntary worker for charity/police etc                          | 16  | 5%   |
| Other                                                            | 70  | 22%  |
| Total                                                            | 334 | 100% |

References

AARP (2003). Off the hook: Reducing participation in telemarketing fraud. ([https://assets.aarp.org/rgcenter/consume/d17812\\_fraud.pdf](https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf)).

AARP (2019). The impact of training financial professionals to prevent financial exploitation. (<https://drive.google.com/file/d/1jc6vl06A-SsBZGZHjWqeQDUX9StBCU8q/view>).

Arizona State University Center for Problem Orientated Policing (n.d.) Situational Crime Prevention Evaluation Database. (<https://popcenter.asu.edu/content/situational-crime-prevention-database-home>).

Bailey, J., Taylor, L., Kingston, P., Watts, G., 2021. Older adults and “scams”: evidence from the Mass Observation Archive. *J. Adult Prot.* 23 (1), 57–69. <https://doi.org/10.1108/JAP-07-2020-0030>.

Bajaj, P., Edwards, M., 2023. Automatic scam-baiting using ChatGPT. 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 1941–1946. <https://doi.org/10.1109/TrustCom60117.2023.00264>.

Burke, J., Kieffer, C., Mottola, G., Perez-Arce, F., 2022. Can educational interventions reduce susceptibility to financial fraud? *J. Econ. Behav. Organ.* 198, 250–266.

Burnes, D., Henderson, C.R., Sheppard, C., Zhao, R., Pillemer, K., Lachs, M.S., 2017. Prevalence of financial fraud and scams among older adults in the United States: a systematic review and meta-analysis. *Am. J. Public Health* 107 (8), 1295. <https://doi.org/10.2105/ajph.2017.303821>.

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. *Polic. A J. Policy Pract.* 15 (3), 1758–1772.

Button, M., Blackburn, D., Sugiura, L., Shepherd, D., Kapend, R., Wang, V., 2021. From feeling like rape to a minor inconvenience: Victims’ accounts of the impact of computer misuse crime in the United Kingdom. *Telemat. Inform.* 64, 101675.

Button, M., Hock, B., & Shepherd, D. (2022). *Economic crime: From conception to response*. Routledge.

Button, M., Hock, B., Shepherd, D., Gilmour, P., 2023a. Understanding the rise of fraud in England and Wales through field theory: blip or flip. *J. Econ. Criminol.* 1, 100012. <https://doi.org/10.1016/j.jecon.2023.100012>.

Button, M., Hock, B., Shepherd, D., Gilmour, P., 2023b. What really works in preventing fraud against organisations and do decision-makers really need to know? *Secur. J.* 37, 965–983. <https://doi.org/10.1057/s41284-023-00402-4>.

Button, M., Karagiannopoulos, V., Lee, J., Suh, J.B., Jung, J., 2024c. Preventing fraud victimisation against older adults: Towards a holistic model for protection. *Int. J. Law Crime. Justice* 77, 100672.

Button, M., Lewis, C., Tapley, J., 2014. Not a victimless crime: the impact of fraud on individual victims and their families. *Secur. J.* 27, 36–54.

Button, M., Shepherd, D., Hawkins, C., Tapley, J., 2024a. Disseminating fraud awareness and prevention advice to older adults: perspectives on the most effective means of delivery. *Crime. Prev. Community Saf.* 26, 385–400. <https://doi.org/10.1057/s41300-024-00218-3>.

Button, M., Shepherd, D., Hawkins, C., Tapley, J., 2024b. Fear and phoning: telephones, fraud, and older adults in the UK. *Int. Rev. Vict.* 31 (1), 117–134. <https://doi.org/10.1177/02697580241254399>.

Button, M., Shepherd, D., Hawkins, C., Tapley, J., 2025. Fear of fraud amongst older adults: a hidden epidemic? M. Button et al. *Secur. J.* 38 (1), 44.

Chouhan, N., Kediya, S., Wagh, U., Deshpande, P., Karmore, P., Das, D., 2024. A Meta-Analysis of AI in Fraud Detection: Evaluating the Effectiveness of Different Algorithms and Data Sources. 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI). IEEE, pp. 1–7. <https://doi.org/10.1109/IDICAIEI61867.2024.10842759>.

Cooper, M., Avery, L., Scott, J., Ashley, K., Jordan, C., Errington, L., Flynn, D., 2022. Effectiveness and active ingredients of social prescribing interventions targeting mental health: A systematic review. *BMJ Open* 12 (7). <https://doi.org/10.1136/bmjopen-2021-060214>.

Cross, C., 2016. Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Crim. Justice Stud.* 29 (2), 125–142. <https://doi.org/10.1080/1478601X.2016.1170278>.

Cross, C., 2020. Oh we can’t actually do anything about that’: the problematic nature of jurisdiction for online fraud victims. *Criminol. & Crim. Justice* 20 (3), 358–375.

Cross, C., 2021. Theorising the impact of COVID-19 on the fraud victimisation of older persons. *J. Adult Prot.* 23 (2), 98–109.

Cross, C., Blackshaw, D., 2015. Improving the police response to online fraud. *Polic. A J. Policy Pract.* 9 (2), 119–128.

DeLiema, M., Shadel, D., Pak, K., 2020b. Profiling victims of investment fraud: Mindsets and risky behaviors. *J. Consum. Res.* 46 (5), 904–914.

DeLiema, M., Deevy, M., Lusardi, A., Mitchell, O.S., 2020a. Financial fraud among older Americans: Evidence and implications. *J. Gerontol. Ser. B Psychol. Sci. Soc. Sci.* 75 (4), 861–868. <https://doi.org/10.1093/geronb/gby151>.

DeLiema, M., Robb, C.A., Wendel, S., 2025. What does trust have to do with it? Training consumers to detect digital imposter scams. *J. Financ. Crime.* 32 (1), 77–97.

Derakhshan, A., Harris, I.G., Behzadi, M., 2021. Detecting telephone-based social engineering attacks using scam signatures. *Proc. 2021 ACM Workshop Secur. Priv. Anal.* 67–73.

Edwards, M., Peersman, C., Rashid, A., 2017. Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. *Proc. 26th Int. Conf. World Wide Web Companion* 1291–1299.

Global Anti-Scam Alliance (GASA) (2025) Global State of Scams 2025. GASA.

Goldstraw-Wright, J., Gill, M., & Button, M. (2024). Enhancing police resources in the fight against economic crime cost effectively: harnessing the potential of the private and not-for-profit sectors: Report for the Dawes Trust.

Her Majesty’s Inspectorate of Constabulary, Fire and Rescue Services HMICFRS (2019). *Fraud: Time to choose.* (<https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf>).

Home Office (2023) *Fraud Strategy: Stopping scams and protecting the public.* ([https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud\\_Strategy\\_2023.pdf](https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf)).

Hong, B., Connie, T., Goh, M.K.O., 2023. Scam calls detection using machine learning approaches. 2023 11th International Conference on Information and Communication Technology (ICoICT). IEEE, pp. 442–447.

Jensen, R.I.T., Gerlings, J., Ferwerda, J., 2024. Do awareness campaigns reduce financial fraud? *Eur. J. Crim. Policy Res.* 1–36. <https://doi.org/10.1007/s10610-024-09573-1>.

Karagiannopoulos, V., Kirby, A., Oftadeh-Moghadam, S., Sugiura, L., 2021. Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Comput. Law & Secur. Rev.* 43, 105615. <https://doi.org/10.1016/j.clsr.2021.105615>.

Kemp, S., Erades Pérez, N., 2023. Consumer fraud against older adults in digital society: Examining victimization and its impact. *Int. J. Environ. Res. Public Health* 20 (7), 5404.

- Kim, S.H., Park, E.S., Lee, S.K., Cho, Y.I., 2025. The Incremental Effects of Fraud Crime on Suicide Among the Elderly in South Korea's Aging Society. *Sage Open* 15 (4), 21582440251385886.
- Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., Kaaria, L., 2023. Can you spot a scam? Measuring and improving scam identification ability. *J. Dev. Econ.* 165, 103147.
- Lazarus, S., 2024. Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity. *Deviant Behav.* 1–25.
- Lazarus, S., Whittaker, J.M., McGuire, M.R., Platt, L., 2023. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000–2021). *J. Econ. Criminol.*, 100013.
- Mills, W.L., Roush, R.E., Moye, J., Kunik, M.E., Wilson, N.L., Taffet, G.E., Naik, A.D., 2012. An educational program to assist clinicians in identifying elder investment fraud and financial exploitation. *Gerontol. & Geriatr. Educ.* 33 (4), 351–363. <https://doi.org/10.1080/02701960.2012.702164>.
- Neighbourhood Watch. (n.d.). Doorstep scams. (<https://www.ourwatch.org.uk/crime-prevention/crime-types/scams-and-fraud/protecting-against-scams/doorstep-scams>).
- Office for Health Improvement & Disparities. (2022, January 27). Social prescribing: applying All Our Health. GOV.UK. (<https://www.gov.uk/government/publication/s/social-prescribing-applying-all-our-health/social-prescribing-applying-all-our-health>).
- ONS. (2020). Nature of fraud and computer misuse in England and Wales: year ending March 2019. (<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019>).
- ONS. (2021). Internet users, UK: 2020. (<https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020>).
- ONS. (2023). Nature of fraud and computer misuse in England and Wales: appendix tables. (<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables>).
- Police Foundation. (2018). More than just a number: Improving the police response to victims of fraud. (<https://www.police-foundation.org.uk/publication/more-than-just-a-number-improving-the-police-response-to-victims-of-fraud/>).
- Prenzler, T., 2020. What works in fraud prevention: A review of real-world intervention projects. *J. Criminol. Res. Policy Pract.* 6 (1), 83–96.
- Rosenorn-Lanng, E. and Corbin-Clarke, S. (2020). Exploring the Impact of Call Blockers on User Well-Being Supporting victims of financial fraud. Bournemouth University. (<https://mycouncil.surreycc.gov.uk/documents/s77885/Item%204%20-%20Annex%20C%20-%20NTS%20Impact%20of%20call%20blockers%20on%20user%20well%20being%20Report%202020.pdf>).
- Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., Carstensen, L.L., 2014. Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic Appl. Soc. Psychol.* 36 (3), 272–279.
- Sherman, L.W., Gottfredson, D.C., MacKenzie, D.L., Eck, J., Reuter, P., & Bushway, S.D. (1998). Preventing crime: What works, what doesn't, what's promising. US Department of Justice, Office of Justice Programs, National Institute of Justice. (<https://www.ojp.gov/pdffiles/171676.pdf>).
- Smith, R.G., Akman, T., 2008. Raising public awareness of consumer fraud in Australia. *Trends Issues Crime. Crim. Justice* (349). (<https://www.aic.gov.au/publications/tandi/tandi349>).
- Tetlock, P.E., & Gardner, D. (2016). Superforecasting: The art and science of prediction. Random House.
- Weaver, G., Trevino, L., Cochran, P., 1999. Corporate ethics programs as control systems: influences of executive commitment and environmental factors. *Acad. Manag. J.* 42 (1), 41–57. (<https://www.jstor.org/stable/256873>).
- Wilson, S., Hassan, N.A., Khor, K.K., Sinnappan, S., Abu Bakar, A.R., Tan, S.A., 2024. "A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia". *J. Financ. Crime.* 31 (5), 1140–1155. <https://doi.org/10.1108/JFC-06-2023-0151>.
- Mark Button** Is Professor of criminology at the University of Portsmouth and Co-Director of the Centre for Cybercrime and Economic Crime.
- Vasileios Karagiannopoulos** Is Associate Professor of criminology at the University of Portsmouth and Co-Director of the Centre for Cybercrime and Economic Crime.
- David Shepherd** Is a Senior Lecturer in Economic Crime at the University of Portsmouth.
- Annie Kirby** Is a Research Associate at the Centre for Cybercrime and Economic Crime.
- Julak Lee** Is a Professor of Security at Chung-An University, Seoul, South Korea.
- Joon Bae Suh** Director of Research and Planning, Professor at Korean National Police University, Assan, South Korea.
- Jeyong Jung** Is a Professor of Criminology at the University of Ulsan, Ulsan, South Korea.
- Chol Soo Koh** Director of External Cooperation Director at KFCPA, Special Advisor at Kim & Chang