Meg Hillier MP
Chair of the Committee of Public Accounts
House of Commons
14 Tothill Street
London SW1H 9NB

26 October 2017

Dear Ms Hillier,

Inquiry into the Growing Threat of Online Fraud

Thank you for giving us the opportunity to give evidence to the Committee last week. I thought it might be helpful to set out briefly below some further reflections in light of the Committee's questions, and I attach an annex setting out some factual information and a summary of Age UK's work in this area. We would be happy to provide further information if necessary.

1. Older people's exposure to risk

The Committee pointed out that the most likely victims of online fraud are under 65. This is correct, but in part it probably reflects the fact that at present older people are much less likely to use the internet than the rest of the population. Only two-fifths (41%) of people aged 75+ are recent internet users, compared to four-fifths (78%) of people aged 54-74 and nine-tenths (89%) of all adults.[i]

Our concern is that this lower exposure to risk may change. There is steady growth in the number of older people online: the percentage of people 75+ who have used the internet has doubled since 2011. However, older people may lack the skills to keep safe when using new technology. For example, people aged 75+ are less confident in knowing how to manage access to their personal data online, and less likely to use security features, except for anti-virus packages and passwords.[ii] Finally, some online frauds particularly affect older age groups, such as pensions and investment fraud, dating fraud, and computer software fraud (see Annex).

Age UK
Tavis House
1–6 Tavistock Square
London WC1H 9NA

t 0800 169 80 80
f 020 3033 1000
e contact@ageuk.org.uk
www.ageuk.org.uk

These are just three types of online fraud affecting older people, but they are particularly heartless examples that seek to exploit people's vulnerabilities, such as loneliness and inexperience with technology. As I said in the session, as well damaging victims' financial security, online fraud can be a serious blow to their confidence, deterring them from taking up new technology, increasing their isolation and making daily life even more difficult.

Disconnection
'I'm frustrated. I unplugged my telephone because of all these nuisance calls. I rarely go on the computer. I used to enjoy that.'
Participant in recent Age UK research among scam targets and victims

2. The limits to consumer education

Our recent research among older people showed that they want information on how to protect themselves. At Age UK, we do our best to meet this need, and over the past year, for example, we have sent out over 50,000 printed copies of our information guides on Avoiding Scams and Internet Security. We also work with the Take Five campaign, for example hosting #TakeFiveOverTea events, and have various projects seeking to support those who might be at risk of fraud, and providing support to victims.

However, we know only too well the difficulties of reaching those who most need our support, and the challenge of encouraging behaviour change. Our recent qualitative research showed that those at risk need help 'in the moment' to pause for thought, and suggested behaviours to protect them from scams. They also need to feel that they are not alone and that there are expert bodies that can help. They want to know that there are community partners who they trust and who can provide non-judgemental practical and emotional support, but also, most importantly, official organisations with teeth, such as the police.

Therefore, it is vital that law enforcement agencies and businesses do not lose the focus on disruption and enforcement. It is ineffective, as well as unfair, to put all the focus on the consumer.

3. Is current action enough?

We welcome the recent pickup in activity and the commitment in the Home Office older people's action plan to strengthen their approach to protecting older people from abuse, exploitation and crime. However, it is clear that action to date has been patchy, as the NAO report shows.

Age UK is represented on the victims and susceptibility strand of the Joint Fraud Taskforce. After a slow start, the Taskforce is now finding its feet, and it is a useful form of collaboration, but we would be concerned if it were to drift into becoming an ongoing, low-urgency project that happens behind closed doors. We would like to see clarity on its longer-term role, and it must lead to strong concerted action, with clear lines of accountability.

We have also had meetings with individual banks, but again, we have a concern about the lack of public transparency and challenge. Consumer organisations do not have the detailed technical expertise to find answers to the issues of fraud: while we appreciate that banks do not want to make fraudsters' lives any easier, we do not see any clear incentive for banks to act where they are not held liable for the loss. For this reason, we think the Which? super-complaint was an important initiative, although our preference would be to see the banks take action voluntarily. This is also why we have called for individual banks to publish information on the level of fraud they are experiencing – as an incentive for change.

However, tackling online fraud is not merely a matter for the banking industry. We are also concerned, for example, that online dating agencies are not making full use of their data capabilities to disrupt fraud.

4. What action is needed?

Our top priorities for Government action are therefore:

1. Make fraud a strategic policing priority and strengthen the capacity of all police forces (and Trading Standards, where appropriate) to respond – fraud is now the most common crime.

2. Ensure the Joint Fraud Taskforce has a clear role, is fully transparent and accountable, and comes out promptly with strong recommendations, including commitments to action from banks and other sectors.

3. Track and report regularly on progress – in 2015 the ONS introduced experimental statistics on fraud and computer misuse, providing an invaluable baseline against which to measure progress. The Government should commit to protecting these statistics from funding cuts.

4. Urgently implement recent proposals to tackle pension scams, including the ban on cold calls, and strengthen the ban to cover cold calls relating to any kind of investment.

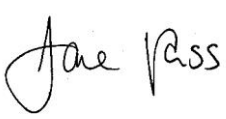
5. Prioritise fraud targeted at the most vulnerable groups, even it is lower-value, and improve partnership working between social services, Trading Standards and police, for example through Adult Safeguarding Boards.

6. Should we see inadequate improvement in bank security, the Government should introduce a formal requirement for individual banks to publish the level of fraud they experience.

Finally, may we point out that while 57 per cent of fraud is cyber enabled, that leaves 43 per cent occurring offline; almost half.[iii] Older people may be especially at risk of such fraud. For example, the average age of postal scam victims is 75. So, we hope that efforts to tackle all kinds of fraud are not de-prioritised in the urgent task to improve our national response to online fraud.

I hope this is helpful.

Yours sincerely,



Jane Vass

Director of Policy & Research

ANNEX

1. Older people and internet use

Older people are much less likely to use the internet than the rest of the population. Two-fifths (41%) of people aged 75+ are recent internet users, compared to four-fifths (78%) of people aged 54-74 and nine-tenths (89%) of all adults.[iv] People of lower socio-economic backgrounds (Table 1), as well as women and people with disabilities, are less likely to be online.

Table 1. Non-internet users, by age and socio-economic background

% NON-INTERNET USERS	All	16-24	25-34	35-44	45-54	55-64	65-74	75+
AB	5%	0%	0%	1%	0%	4%	12%	35%
C1	8%	2%	0%	3%	6%	6%	22%	58%
C2	20%	0%	4%	8%	3%	26%	46%	80%
DE	22%	7%	6%	16%	15%	32%	35%	81%
All	13%	3%	3%	6%	6%	16%	29%	64%

(Source: Ofcom, 2016.[4])

Further, older people who are online undertake fewer activities. For example, they are less likely to make transactions than average (17% v 52% in the last week), use social media (14% v 49%), do their banking (26% v 53%), or shop (15% v 48%).[v]

However, this does not mean older people are not at risk of online fraud. Firstly, there is steady growth in the number of older people online; only 20 per cent of people 75+ used the internet in 2011. Secondly, many older people lack security skills. For example, people 75+ are 1) less confident in knowing how to manage access to their personal data online, and 2) less likely to use security features, except anti-virus packages and passwords.[vi] And thirdly, we are aware of particular online frauds that impact older people, described in the next section.

2. Older people and online fraud

Through Age UK's information and advice service (both our national helpline and local services) we see cases of many different types of fraud, both online and offline, affecting older people. Here we highlight four types of online fraud impacting older people, giving real (anonymised) examples.

i. Pension and investment fraud

The NAO report includes investment fraud as a type of online fraud.[vii] The pension 'freedom and choice' reforms that came into force in 2015 have been followed by a significant increase in pension and investment frauds. People have lost an estimated £43 million to pension scammers since April 2014. People aged 55+ are, by definition, targeted by these frauds and FCA research shows that the chances of being a victim of investment fraud increases with age.[viii] See case study 1.

We welcome the Government's proposals to tackle pension scams.[ix] However, the Government should act quickly to bring the cold call ban into force, and this cold call ban should be extended to cover investment scams, as it will be too easy for fraudsters to find loopholes by not explicitly mentioning pensions.

Case study 1

The client said they had transferred more than £40k from their pension to a Carbon Credits investment company. They have just found out this is a bogus scheme. They asked whether they should report it or is their money lost.

ii. Romance fraud

Fraudsters use fake online dating profiles to groom victims, build trust and defraud them. This is a bigger issue than many may realise: Action Fraud receives around seven romance fraud reports every day. This reflects an increase of 32 per cent over a two-year period (from Jan 2013–15). Victims lose £10k on average and we know of cases where people have lost more than £100k.[x] Almost half (45%) of victims indicated that dating fraud had a 'significant' impact on their health or financial wellbeing.

A quarter of victims are in their 50s and over two thirds are between 40 and 69. Age UK sees cases of victims in their 80s, often through a concerned relative or friend. Victims may be especially vulnerable if they experience isolation or loneliness. See case study 2.

Online dating agencies have a key role to play in identifying fraudsters, warning customers, and providing support to victims.

Case study 2

The client's mother lives in France and has dementia. She has been scammed through an online dating agency and has lost more than £10. The client has tried to address this but their mother denies there is a problem. They want their mother to return to the UK but she doesn't want to, despite being very isolated.

iii. Computer software service fraud

This kind of fraud is the third most reported type, according to Action Fraud. The average loss suffered by victims is £600. It particularly impacts older people – the average age of victims is 62.[xi] See case study 3, below. Like other telephone-based scams, older people may be at risk in part because they are more likely to be at home during the day.

Case study 3

The client's 'elderly' friend has been receiving fraudulent internet support calls. The fraudsters say her computer has a virus and tell her how to remove it, at the cost of more than £100. She thinks this is all 'above board' and does not think it is fraud. The client wants to know what they can do to help their friend.

iv. Bank transfer fraud/vishing

This particular fraud involves fraudsters phoning victims, impersonating their bank or the police and convincing them to transfer large sums to a supposedly 'safe' account or divulging their financial information. The Financial Ombudsman Service reviewed complaints made by victims against their bank, following such a fraud.[xii] It found that the most common type of this fraud involved an online transfer of money, and that people aged 55+ made up more the vast majority (80%) of the victims. See case study 4.

Case study 4 (Direct quote from Financial Ombudsman Service report[xiii])

'Mr H took a call from someone who said they were from the police. He was told that his debit cards had been compromised.

Mr H was convinced by the scam and called his bank's number to check what the "police officer" had said was true. Mr H didn't realise at the time that the fraudster was still on the line and this was a con to get him to disclose personal security information. He was asked to key his PIN into the phone for verification. And while he was still on the phone to the person he thought worked for his bank, a "courier" arrived to take his bank cards away.

Mr H soon started to feel that something was not right – and contacted his real bank the following day. They confirmed that a significant sum had been removed from his savings account and more money had been withdrawn at cash machines.

The bank said they couldn't refund the money because Mr H had been negligent in giving away confidential information.'

These are just four examples of online fraud affecting older people. It is vital our collective response to online fraud improves; as more older people go online over time they may become at risk, particularly if they do not have the skills to be safe online. However, while 57 per cent of fraud is cyber enabled, that leaves 43 per cent occurring offline, almost half.[xiv] Older people may be especially at risk of such fraud. For example, the average age of postal scam victims is 75.

Impacts on older people

Fraud has a harmful impact on older people in a number of ways. In terms of financial losses, many people lose significant sums: we have heard of multiple cases of people losing more than £100k. Some people have had to sell their home as a result. Even relatively small losses can have a devastating impact, destroying life savings and financial security for the future.

Fraud also harms people's physical and mental health, and independence. For example, a study into the impact of doorstep crime on older victims by Greater Manchester Police[xv] showed that their health declines faster than non-victims of a similar age. Evidence also suggests victims may be more likely to require health and social care services they didn't previously need, putting more pressure on the state. The National Trading Standards Scams Team reports that people defrauded in their own home are 2.5 times more likely to either die or go into residential care within a year. See case study 5.

Case study 5

The client's neighbour lived alone and was the victim of a doorstep scammer.

As a consequence, she wouldn't open the door to anyone, leaving her to struggle to look after herself. She had dementia and needed help with washing, dressing, preparing food, etc. She deteriorated to such a degree that another neighbour became concerned, and called an ambulance. She spent six weeks in hospital and is now in a care home.'

3. Age UK programmes

Age UK has a network of around 140 local partners (local Age UKs) around the country. Each one provides an information and advice service, including support for people around income maximisation. A small number of partners run dedicated scams services, for example, Age UK East Sussex supports older scam victims.[xvi]

In 2018, four local partners in London will pilot a new Scams Prevention and Victim Support service, supported by the City Bridge Trust and working in close partnership with Action Fraud. The programme will support over 2,100 vulnerable older Londoners. Local partners will run three core activities: awareness raising sessions for an audience of older people, friends and family; one-to-one sessions for older people who are vulnerable and at risk of scams; and specialist one-to-one support sessions for older victims.

By delivering this work, we aim to:

- raise awareness of scams and the ways in which they can be reported,
- empower older Londoners to feel safer, more secure and more confident;
- prevent older victims of fraud from becoming repeat victims; and
- demonstrate an evidenced model for this work that could be used in other areas of the country.

[i] https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017
[ii] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[iii] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017
[iv] https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017
[v] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[vi] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf
[vii] https://www.nao.org.uk/wp-content/uploads/2017/06/Online-Fraud.pdf
[viii] https://www.fca.org.uk/publication/research/quan-study-understanding-victims-investment-fraud.pdf
[ix] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/638844/Pension_Scams_consultation_response.pdf
[x] http://www.actionfraud.police.uk/news/dating-fraud-victims-report-once-every-three-hours-feb17
[xi] http://news.cityoflondon.police.uk/r/853/city_of_london_police_collaborate_with_microsoft_#
[xii] http://www.financial-ombudsman.org/assets/pdf/vishing-insight-report2015.pdf
[xiii] http://www.financial-ombudsman.org/assets/pdf/vishing-insight-report2015.pdf
[xiv] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017
[xv] http://www.gmp.police.uk/content/se ction.html?readform&s=8034084491 78D82780257961003E0749
[xvi] https://www.ageuk.org.uk/eastsussex/services-we-provide/age-uk-east-sussex-and-edna-johnson-wills-trust-scams-prevention/