Bournemouth University

The National Centre for Post-Qualifying Social Work and Professional Practice

appg All-Party Parliamentary Group on Financial Crime & Scamming

Financial Scamming and Fraud

Working in partnership with:

Burdett Trust for Nursing

City of London

age UK Love later life

cifas Leaders in fraud prevention

National Trading Standards Scams Team

Trading standards

SOLLA Society of Later Life Advisers

ctsi Chartered Trading Standards Institute

Foreword

Fraud and scams are growing crimes. The Office of National Statistics England and Wales Crime Figures showed that 662,519 police recorded fraud offences took place from October 2016 to September 2017, and their Crime Survey showed there were 3.2 million estimated incidents of fraud in the same period.

Fraud is the 21st century volume crime and the issue is not going to go away. With more and more people sharing data, transacting, setting up businesses, dating and chatting online this trend is only going to continue.

That is why in 2017 the All-Party Parliamentary Group on Financial Crime and Scamming was set up. This group acts as a voice in Parliament on scams, fraud and wider financial crime. I am therefore grateful to the National Centre for Post-Qualifying Social Work and Professional Practice at Bournemouth University, who lead the national research in this area of crime on behalf of the National Scams Team and The Chartered Trading Standards Institute, for working with the key national organisations in this field to pull together this information resource pack. It is clear from this research that the issue is massive and is not going to go away without a clear and consistent approach to tackle the problem.

Many frauds and scams are conducted by criminals who are not even in the same county as us or even the same country. It is a crime we will find difficult to arrest our way out of; therefore we all need to take steps to help prevent this crime against ourselves, our families and our communities.

I commend this resource to my Parliamentary colleagues and to all in society who want to join with us to help eradicate financial scams and fraud.

Conor Burns M.P.

Chair APPG - Financial Crime and Scamming

May 2018

Foreword

Financial scamming and its impact have been receiving a higher public profile in recent months, yet though it is recognised as a growing problem, there is a lack of clear research and evidence into the scale of the problem, its causes and the impact on the public.

The National Centre for Post-Qualifying Social Work and Professional Practice at Bournemouth University have been working with key national organisations in the UK to develop a better understanding of this issue, seeking ways and solutions to reduce the risk of financial scamming.

I want to thank the many organisations who have shared their experience and data with us to help formulate our thoughts and understanding. In particular, The National Trading Standards Scams Team, Chartered Trading Standards Institute, North Yorkshire Trading Standards, The City of London Trading Standards Team, CIFAS, Grant Thornton, STOP the Loan Sharks and The Burdett Trust for their help in funding part of this research.

We are continuing to work with these bodies, plus other leading agencies in this field, to develop a clearer understanding of the scale and impact of scams and their implications for society.

This document has been updated from our original work in order to support the work of the All-Party Parliamentary Group chaired by Conor Burns M.P.

What is clear is that the range, scope, impact and amount of financial scamming and fraud is simply enormous. Its impact on individuals, families and society is devastating and we simply must do more to prevent, protect and stop this crime wave.

Although it is clear that everybody is a potential victim to this type of crime, we need to remember that the criminals are very clever and use significant resources in order to commit financial scams and fraud. It is apparent that those at greatest risk are lonely, older people and, specifically, those with a cognitive impairment (dementia) who may be unable to safeguard themselves as a result of their health or social care needs.

This work is far from complete and we are continuing to research and develop our ideas and understanding. If you would like to contribute your thoughts or ideas please contact me. It is only via our collective efforts that we will be able to tackle this growing issue and we positively welcome your input and support.

Professor Keith Brown
Director

The National Centre for Post-Qualifying Social Work and Professional Practice

Bournemouth University
4th Floor, Royal London House
Christchurch Road
Bournemouth
Dorset
BH1 3LT UK

Tel: 01202 964765
Fax: 01202 962025
pqsw@bournemouth.ac.uk
www.ncpqsw.com
@researchpqsw

We asked....

1

All agencies, especially financial institutions, should:

- Recognise that consumers/clients with dementia are at risk of being scammed. Therefore, measures to protect this population group are required as part of a 'duty to care', and those with a diagnosis of dementia have, by definition, a cognitive impairment which means that their potential 'unwise decision' may be a result of their cognitive state rather than simply an unwise decision.

2

All organisations that hold personal data should:

- Only share or pass on personal details and information to other organisations via a clear opt-in as opposed to an opt-out process. Data should only be held for a maximum of 12 months before permission needs to be sought again.
- Recognise that the normal default position should be that charities do not share, pass on or sell personal details to help prevent 'Suckers Lists'. The exception being to report a safeguarding concern to statutory agencies where there is a suspicion that the person(s) is/are at risk of harm or scamming and this information should be used in accordance with The Care Act (2014).

3

Citizens who feel at risk of financial scamming should be able to:

- Formally notify their bank or building society in writing stating that they feel at risk and requesting that all transactions to new payees above a defined threshold (perhaps £1000) have a 24-hour delay before being processed.
- At the start of the 24-hour delay period, an email/text alert is automatically sent to the customer's nominated representative (relative/friend) stating that the customer is attempting to make a large transaction. This will give the opportunity for the proposed transaction to be challenged with a view to potentially stop it from leaving the consumer's account.

We did....

1

We have delivered over 20 radio and television broadcasts and 15 national conference keynote addresses. We have published the national guidance on Lasting Powers of Attorney in relation to next of kin and the National Mental Capacity Act Competency Framework. These documents provide key information and raise awareness of issues related to capacity and decision making. In addition we published a new text book: Safeguarding adults, financial scams and mental capacity. The Chair of CTSI has issued this text as national guidance to every trading standards team, and a copy has been provided to every safeguarding adult board.

There is still much to do as those with cognitive impairments are a group at significant risk of fraud and scams and we will continue to raise awareness.

2

The new General Data Protection Regulation (GDPR), which comes into effect on 25.5.18, is a significant step to prevent unauthorised data sharing and to stop 'suckers lists' at source. Awareness raising amongst the general public and organisations is necessary to increase understanding about the importance of GDPR in preventing scams and fraud.

We are working in partnership with the Joint Task Force (JTF) and National Trading Standards Scams Team to raise awareness of data protection. We have produced learning materials for Age UK and the community health sector which are being promoted by NHS England's safeguarding team to help alert healthcare professionals to scam prevention and data protection.

3

We will continue to push financial institutions to develop systems which actively protect customers made vulnerable by their health or circumstances.

'Self-declaration' or vulnerability should and must trigger systems designed to prevent financial fraud and we will work in partnership with CIFAS and the financial sector to achieve this.

We will continue the ongoing work with the City of London Police, Action Fraud and the City of London Corporation to promote awareness amongst financial institutions and seek further protective measures for their customers.

We supported the JFT to launch the British Standards Institution's PAS standardisation system and to implement a working group focused on banking interventions.

2018 asks

1 Challenge to financial institutions:

All financial institutions should set out the steps they will take to identify customer susceptibility to fraud and scams and implement appropriate protective measures.

- Publishing performance data so customers can hold financial institutions to account.
- Adoption of the British Standards Institute's code of practice.
- Continuation of partnership work with the Joint Fraud Taskforce. and active pursuit of systems to stop fraudulent payments and block fraudulent but authorised push payments.
- A strong focus on prevention by all financial institutions through raising awareness and staff training on recognising signs of scam and fraud susceptibility
- Adopting initiatives such as Friends Against Scams.

2 Challenge to government:

The government should publish a joint strategy on fighting fraud and reducing harm to the public from fraud and scams. This strategy should:

- Be shared across all government departments that have responsibility for fraud, scams and financial abuse (including the Home Office, the BEIS and the DCMS).
- Set out methods of sharing best practice and ensuring consistent messaging across all sectors.

The aim: to reduce duplication and confusion and enable joint commitment to fight fraud.

3 Challenge to local government:

Local authorities should ensure they have strategies to tackle fraud which link relevant services, including Safeguarding Adult Boards and adult social care, trading standards public health.

These strategies should include:

- Action supporting individuals and improving their wellbeing.
- Prevention of harm from abuse
- Intelligence sharing, disruption of criminal activity and law enforcement

4 Improve fraud awareness in the next generation:

One of the fastest growing groups of people responding to scams is young people aged under 25.

To upskill future generations we believe financial education should be a compulsory part of the school curriculum from Key Stage 3 to include:

- Fraud and scam awareness
- Financial literacy skills

Key Points

Scam is a slang term for personal fraud. The financial sector considers involvement in scams to be the responsibility of the individual, whilst fraud is beyond the individual's responsibility.

Financial scamming can affect anyone. It is vastly under reported and the true scale of the financial loss and other impacts is unknown.

Factors such as loneliness, social isolation, poverty and cognitive impairment can make people more vulnerable to responding to financial scams or fraudulent schemes.

Older people are targeted by certain types of scams such as doorstep, mail, telephone and investment scams.

Cognitive impairments, such as dementia, can interfere with an individual's financial capacity. Those with dementia may not have the skills to judge risk and can find it more difficult to apply precautionary measures to decision making which puts them at increased risk of responding to a scam.

Financial fraud and scams have been an issue for many years, but the internet and increasing use of e-commerce has accelerated the problem.

Many people who have responded to a scam are put onto 'suckers lists'. These lists are sold globally between fraudsters.

The term 'adults at risk of neglect and abuse' is now used within adult safeguarding policy which moves the focus from notions of vulnerability, which has been associated with blaming the individual.

An ageing population is likely to put pressure on the health and social care economy. These services are already struggling to manage the present demand. Older victims of financial crime will experience loss of assets and may become financially dependent on the state for funding future care needs.

Financial scamming has seriously damaging consequences for individuals and society. The impact is often underestimated. Falling victim to a scam can be a life-changing event undermining health, wellbeing and quality of life.

What is the problem?

New data regarding fraud victimisation is now collected by the annual ONS Crime Survey for England and Wales and informs calculations made by the Annual Fraud Indicator (2017) that personal fraud cost an estimated £6.8 billion in 2016. This figure includes £4.5 billion lost to mass marketing fraud and £1.3 billion to identity fraud but does not include doorstep crime. The loss indicates the significant impact of personal fraud or scams on individual and societal wealth, reducing personal wealth, consumer confidence and money spent within the UK as many scams involve money being sent abroad (Lonsdale et al. 2016).

Financial abuse from scamming

The Care Act (2014) recognises the risk posed to individuals and society from financial abuse and identifies scamming as a specific form of abuse. The Care Act imposes duties on Local Authorities to prevent and protect citizens from abuse and neglect (Care Act, 2014 Section 1(3)).

Financial abuse from scamming causes serious detriment to individuals and society, and if we fail to respond appropriately to the threat by safeguarding those at risk through prevention, early intervention and the prosecution of perpetrators it is likely that the financial and social impact will only grow.

What is financial scamming?

Fraud involves a person dishonestly and deliberately deceiving another person for personal gain, such as property or money and involves situations where a person makes a representation that they know to be untrue or misleading. This includes a range of activity such as online shopping and auction scams, lottery scams and investment fraud (ONS 2016). Crime statistics for England and Wales reveals that the most prevalent form of fraudulent activities are banking and payment card frauds which usually involve falsely obtaining personal bank or payment card details in order to carry out fraudulent transactions (ONS 2018).

Estimates derived from the new fraud and computer misuse offence questions show there were 4.7 million incidents in the latest Crime Survey for England and Wales (ONS 2018).

The 'success' of scams rely on the individual choosing to respond or participate. To make the transaction appealing scammers utilise business skills using techniques of persuasion and legitimate marketing. (Carter 2017).

The average age of individuals on 'suckers lists' was 75.

(National Trading Standards 2016)

What is a 'suckers list'?

The personal details of people who have responded to a scam are then put onto 'suckers lists'. These lists are sold globally between fraudsters who are looking to target vulnerable people. The selling of 'suckers lists' can lead to people being repeatedly targeted by scams.

The details recorded in these lists will vary but can include names, contact details, dates of birth, age, items bought, types of scams previously responded to and amounts of money handed over to scammers.

The National Trading Standards Scams Team have accessed 15 'suckers lists' to date, obtained from various different sources and partners. These lists contain over 300,000 names.

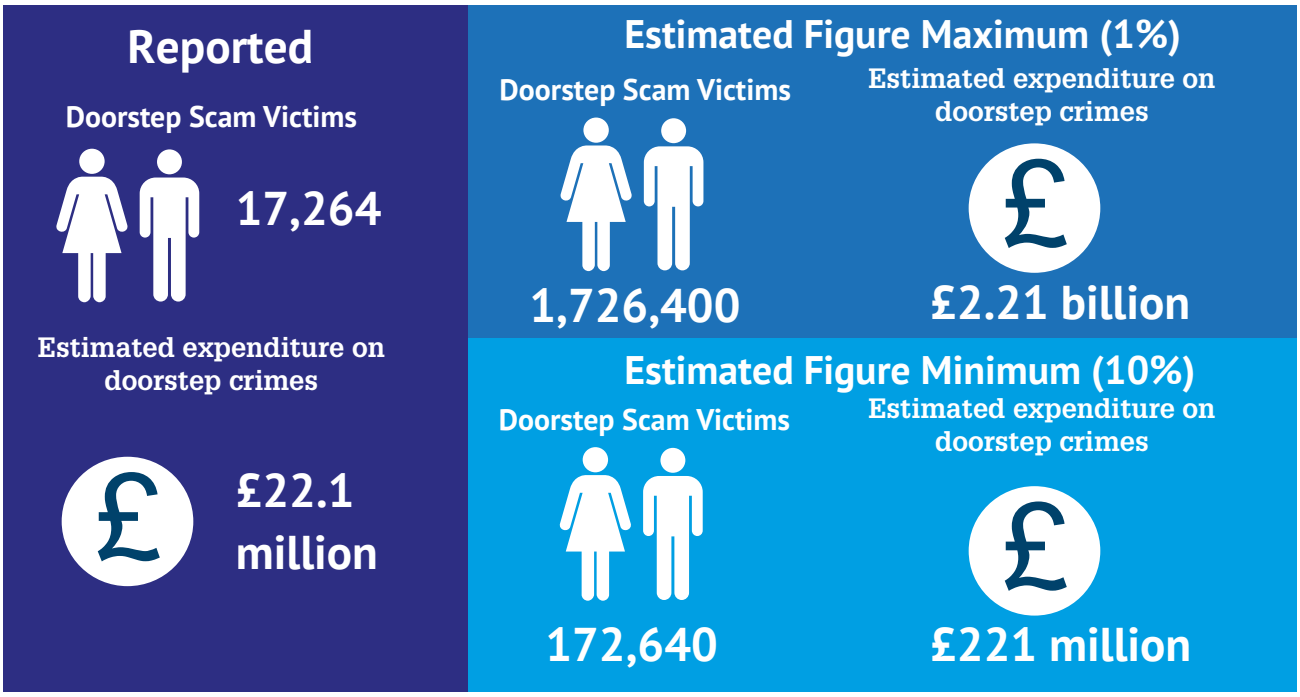
How big is the problem?

The true financial loss resulting from scams is difficult to calculate due to underreporting and agencies collating data relevant to their expertise, for example Financial Fraud UK identified £768.8 million in fraud losses across payment cards, remote banking and cheques in 2016. This is an increase of 2 per cent compared to 2015 and does not include doorstep crime or mass marketing fraud (Financial Fraud Action UK 2017). The rise is attributed to the growth of impersonation, deception scams, online attacks such as malware and data breaches (Financial Fraud Action UK 2017). Underreporting means the true scale is unknown. For example, it is estimated that only 1-10% of doorstep scams are reported (ACTSO 2015).

The National Trading Standards Scams Team calculate that financial scams annually cost UK citizens and the economy between £5-10billion.

Doorstep Scams in England (2014-2015)

"Reporting levels of doorstep crime are believed to be between 1% - 10%"



Why is it underreported?

Individuals may be reluctant to report involvement in scams due to embarrassment or concerns that their financial loss is too insignificant to be investigated seriously. Scammers commonly target small amounts of money from large numbers of people as insignificant loss is less likely to be reported. Scams are vastly underreported, and are less frequently reported by older people (James, Boyle and Bennett 2014). Low levels of reporting make it difficult to achieve accurate information about the scale of financial scamming and, as a result, reported figures are likely to represent only the tip of the iceberg and the true detriment could be much higher.

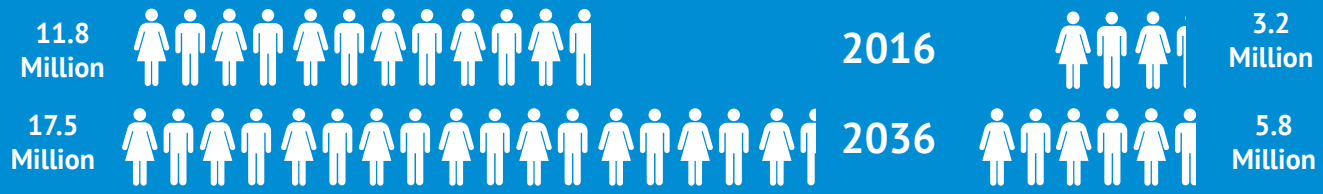
Is scamming a growing problem?

Different types of financial scams have been taking place for many years. However, an increase in use of the internet and e-communications for mass marketing fraud has given fraudsters a new way to target a global audience (Chang 2008). This has provided fraudsters with the opportunity to collate information into 'suckers' lists' which are easily sold on the web to other scammers.

How big will the problem get?

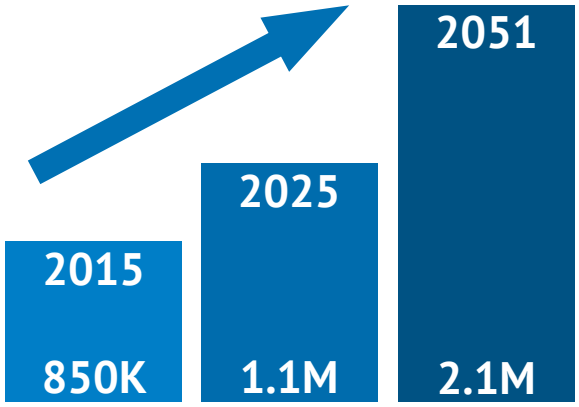
We are all potentially vulnerable to responding to scams and fraud. Scammers use sophisticated language and marketing techniques to appear genuine and authoritative, creating different scams to appeal to different audiences (Carter 2017). Whilst CIFAS reports that 31-40 year olds are the most reported age group of scam respondents with the under 25's being most likely to respond to online banking scams (Citizens Advice 2014), factors associated with older age such as bereavement, cognitive impairment, or social isolation and poverty can increase susceptibility to responding to scam approaches (Age UK 2015). The UK population is ageing which means the proportion of older to younger people will also increase. This places pressure on services to meet the growing need.

The Office of National Statistics Population Projections for the UK



(ONS 2016)

Alzheimer's Society projections of the UK population living with dementia



If current trends continue and no action is taken, the number of people with dementia in the UK is forecast to increase to 1,142,677 by 2025.

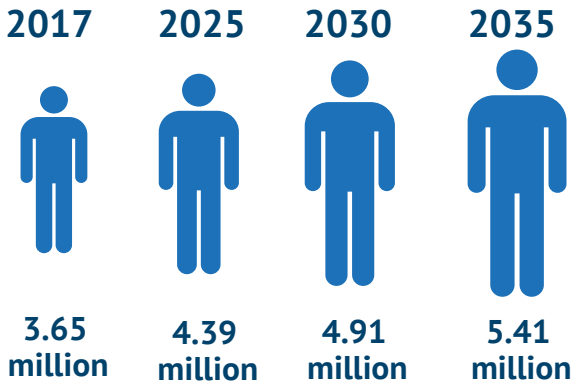
(Alzheimer's Society 2016)

An ageing population that is increasingly living alone may also indicate increased numbers of older people at risk of financial scams.

In 2017, 67% of people who were living alone were female, in comparison to 33% of males.

The demand and costs for health and social care are likely to increase over time as the population ages. Older people who lose savings to scams will be unable to contribute to their care costs in old age resulting in higher costs to state-funded provision.

Population predictions for people over 65 living alone in England



(Poppi 2017)

What impact does scamming have?

Financial scamming can have seriously damaging consequences on individuals and society. The impact is often underestimated. Becoming involved with a scam can be a life-changing event.

Individuals

The financial loss can range from a few pounds to hundreds of thousands of pounds, depending on the type of scam and the number of times an individual has responded. In many cases the financial loss is severe enough to impact an individual's wellbeing and day-to-day standard of living. Scam respondents may go without food, sell or re-mortgage their home or take out loans to fund scams or debts caused by scams.

Scams can cause long lasting or permanent damage to an individual's health and quality of life. Many individuals experience injury to their confidence and trust, and some people are left with the psychological effects of stress, anxiety, fear, depression and shame. Individuals may deny their involvement and others may blame them.

Scams can be a major factor in the decline of health in older people. The Home Office carried out a study in 2003 on burglary and it was reported that older victims of doorstep crime decline in health faster than non-victims of a similar age (Donaldson 2003).

Case Study

Mrs. M began responding to prize draw scams, sending £10-£15 regularly to 'win' the money to pay off her daughter's debts. This could bring her daughter home from overseas. Over 15 years Mrs. M spent her life savings, over £20,000, on scams and admitted she had become addicted to responding. She became seriously ill, couldn't work and lived off benefits. Mrs. M went without food to fund the scams and showed Trading Standards Officers empty food cupboards and piles of daily scam letters. Whilst recovering from a stomach operation, Mrs. M survived purely on liquid supplements supplied by the hospital. She accrued a debt of £2,000 to her bank.

Society

Scamming causes financial detriment to both individuals and wider society. Scamming increases the pressure on public services who have a duty of care to safeguard individuals from financial abuse. The Care Act (2014) recognises the significant threat that financial abuse poses to adult health and wellbeing and places a responsibility for protection on local authorities.

Loss of assets and finances may result in individuals being unable to contribute to their health and social care costs in older age, increasing the financial burden on society for future care provision.

People with dementia are particularly at risk of financial abuse and scamming, and this puts additional pressure on community and residential dementia care services.

With more scam victims losing large sums of money, there is more pressure on public funding. Financial scamming will continue to be a challenge for the economy if it is not tackled in the future. Scams can undermine the health and wellbeing of victims resulting in increased demand for health and social care support.

Why do people respond to scams?

Most of the research into financial scamming to date has focused on the reasons why people respond to scams. This includes understanding the persuasive techniques used by scammers to encourage responses, the process of grooming an individual to respond to a scam and the characteristics of individuals which make them more susceptible.

Persuasive techniques used by scammers

Scammers and fraudsters are skilful at using persuasive techniques of marketing and communication. They encourage individuals to make decisions based on emotional or visceral responses which can result in quick and unwise decision making. Techniques similar to those seen in cases of sexual exploitation may be used to groom scam victims such as frequent, attentive contact with small rewards reinforcing the relationship. The grooming may continue for significant periods before the individual loses any money.

The more proximate the reward, the greater the visceral response will be.

(Langenderfer and Shimp 2001)

Believing a scam or fraud is actually a genuine offer or opportunity is a key factor in scam involvement (Olivier et al. 2015). Research has identified four primary psychological processes used by scammers to encourage compliance:

Deterioration of decision making with incentive

The potential to win a large amount can lead to ineffective decision making, particularly when faced by a scam offering a financial windfall which is just too tempting (Ariely, et al. 2009). People with cognitive impairment may be particularly vulnerable to this type of scam.

Acceptance of cues that create trust

Scammers use different techniques to elicit trust, including legitimate names and logos, faked customer reviews, positions of authority and common ground. People who put more importance on the interpersonal interaction than the details of the offer will miss the scam cues.

Social influence and consistency

People influence other's behaviour in different ways, including conforming to behaviour, reciprocating offers and gestures and being consistent in actions. Establishing similarity with potential victims or repeatedly asking for payments are a manipulation used in scams.

Urgency and scarcity

Scams which require immediate response to claim a prize increase the likelihood of scam involvement. Scams which create a sense of urgency or scarcity prompt visceral responses linked to reduced impulse control, and this may be particularly heightened when faced with large potential gains (Knutson and Samanez-Larkin 2014).

(Fischer, P., Lea, S. and Evans, K. 2013)

Scammers appeal to basic human needs and motivations such as opportunities which lead to financial security or companionship which invoke emotional or visceral responses. Visceral responses may stop individuals from thinking about the scam for long enough to consider the risks or credibility.

Individual Characteristics

Most people will have received some form of scam correspondence, but not everyone responds. Respondents appear to be more open to persuasion particularly by people they do not know.

Involvement in scams may also provide the respondent with a sense of utility through engagement with meaningful activity, and a sense of purpose (Olivier, Burls, Fenge and Brown 2015). This can make respondents reluctant to give up their involvement.

Urgency and scarcity

Some people are more vulnerable to the pressure put on by scammers. People who struggle to make decisions under pressure are likely to be more vulnerable to scams.

Consistency and commitment

Scammers may ask for small steps of compliance such as regular payments or contact. People who are comfortable with routine and consistency are likely to respond to such scams.

Gambling rewards

Some people view scams as a gamble and are prepared to pay the relatively small costs for the chance to gain high rewards. The relationship between costs and rewards, the susceptibility to gambling, can make people more vulnerable to scams.

Emotional control

Some victims have less control over their emotions compared with non-victims. People who struggle to regulate their emotional attachment are likely to be more vulnerable to scams.

(Office of Fair Trading 2009)

What individuals had to say

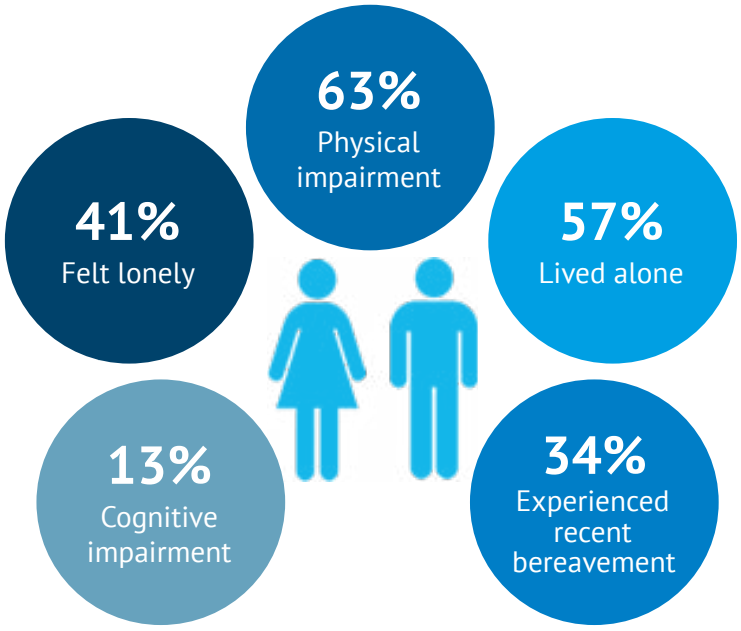
> "It gave me something to do, take my mind off ... Like a little job, because I had nothing else."

> "They play on that you see, your emotions and everything. It wasn't until sometime after my husband died that I really began to get involved with it because it gave me, I know this sounds silly, something to take my mind off my grief."

> "They kept saying we can wait, there is no hurry, we understand. We're sorry for your loss. They were comforting me in one way, it's ridiculous to say it you know, quite friendly and believable. Took me over really."

(Olivier, Burls, Fenge and Brown 2015)

Victim Profile:
The Doorstep Crime Victim Impact Survey



(National Trading Standards Board, 2015)

Who is at risk from scamming?

53% of people aged over 65 believe they have been targeted by a scam or fraud (Age UK 2015). Scammers design schemes to appeal to specific groups and will customise the style and content of the fraudulent scheme to fit the profile of those targeted.

This could mean that a staggering half a million older people have fallen victim to losing savings.

(Age UK 2015)

People may respond to scams and fraud because scammers reinforce messages and strengthen the appearance of authenticity by combining scam types; for example, linking bogus sales with prize draws, or using multiple communication techniques such as cold calls followed by post or emails. This can have a persuasive effect on individuals. Many people do not recognise that they have been targeted by scammers or that they have responded to a scam or fraudulent approach.

65% of doorstep scam victims were aged 75 and over.

(National Trading Standards Board 2015)

Those most at risk of financial scams include:

- Older people who may be targeted by particular types of scams including consumer fraud, telephone and mail contests, and get rich-quick investment schemes (Crosby et al. 2008).
- People who are socially isolated are at increased risk of responding to scams because of having fewer opportunities to meet with others to discuss finances, scams or their decisions with others (Age UK 2015).
- Those with dementia and cognitive impairment may lack financial literacy skills and judgement. It is also difficult to detect scams and financial abuse in people who have dementia because of a lack of confidence in their credibility (Alzheimer's Society 2011).

Risk Factors...more information

Loneliness

Loneliness is a significant issue for society with increasing recognition of the profound impacts of loneliness on health and wellbeing (Age UK). Both loneliness and social isolation have been identified as contributory factors to susceptibility to scams and fraud, with socially isolated older adults being particularly susceptible to financial scams (Lubben et al. 2015).

"Over one million older people said they always or often feel lonely"

(Age UK 2014)

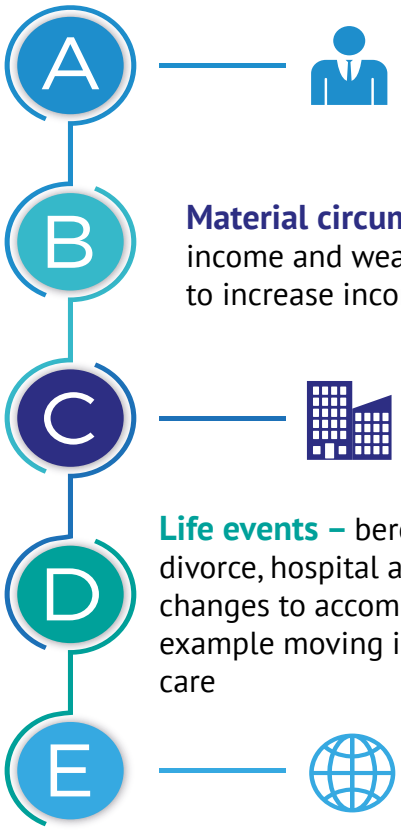
Loneliness and social isolation are experienced differently and people who are socially isolated may feel lonely, whilst those who feel lonely may not be socially isolated (Luo et al. 2012).

Social isolation is an objective term used to describe a lack of contact with others including friends, family and the community.

Loneliness is a subjective term used to describe how a person feels about themselves and how their contact with others differs from their desired social interaction.

Older adults may experience increased levels of loneliness and social isolation due to life events and change reflected in the following psycho-social factors (Victor et al. 2005):

Socio demographics – ageing, changes to family structures such as relationship breakdown



Material circumstances - income and wealth, opportunity to increase income

Health – changes to health and wellbeing such as disability, cognitive impairment and mental health impacting on the ability to initiate and maintain social relationships and engage with the wider community

Life events – bereavement, divorce, hospital admission and changes to accommodation for example moving into residential care

Social resources – changing friendships, family, community activities and contact, time spent alone

Whilst experiences of loneliness and social isolation are not exclusive to older adults, the above factors increase the likelihood of older people living alone and having reduced social contact. Loneliness can impact on health, wellbeing and quality of life. Chronic feelings of loneliness can lead to health problems including poor sleep, memory problems, increased blood pressure, cardiovascular disease, depression, anxiety and feelings of worthlessness (Age UK 2016).

3 in 10 of those aged 80 and over report being lonely

(Office of National Statistics 2015)

Social isolation and loneliness leaves people without support, and for some people their only form of social contact is market-based communications such as telemarketing phone calls and scam mail. Responding to these calls or mail creates a relationship which can become strong as the frequency, and reliability of the contact becomes more highly valued than the quality of the contact (Kang and Ridgway 1996). These relationships can be experienced by the individual as socially supportive and can have a positive impact on health and well-being. This means that it is not easy for the individual to stop their involvement in the scam if there is nothing to take its place.

Half of people aged over 65 said the television or pets are their main form of company.

(Age UK 2014)

9% of older people feel trapped in their own homes.

(Office of National Statistics 2015)

People who do not have a social network can find it difficult to talk to others about their finances or have the opportunity to discuss 'offers' or 'schemes' with other people. Socially isolated individuals may not be aware of current scams in their local area and there are fewer opportunities for other people to notice, identify or intercept scams targeted at the isolated person.

Case Study

Mr. G is 67 and has lived alone since his wife died. Awaiting a hip replacement, he has poor mobility and cannot drive. Mr. G received clairvoyant scams after the loss of his wife and he responded because he felt lonely. He then started receiving and responding to prize draws and catalogue scams until he got caught up in a daily routine of repeat orders to pass the time.

After intervention from Trading Standards, it emerged that Mr. G had £41,000 of debt across five credit cards he had taken out to fund scams. Wardrobes and cupboards in his house were stacked with goods that were of no use to him.

Case Study

Ms. X is in her mid-70's and has been replying to clairvoyant scams for over 20 years following the loss of her husband. Although Ms. X remains fairly active and has a family, her family do not visit and responding to clairvoyant letters helps her with feelings of loneliness. Ms. X received 10-15 scam letters per week, sometimes more, and encloses between £10-40 in every response, the majority of her disposable income.

Trading Standards have attempted to intervene but Ms X gets comfort from the frequent 'social' scam contact and chooses not to stop responding.

Dementia

Dementia is an umbrella term for conditions associated with the decline in cognitive abilities which may interfere with everyday life. Symptoms of dementia include memory loss, difficulties with communication, problem solving and reasoning. It is a progressive condition affecting an individual's abilities and mental capacity over time. Globally there are 47.5 million people with dementia (World Health Organisation 2016). 'It is important that all public services consider the impact of dementia on safeguarding adults activity and how the condition may increase vulnerability to financial abuse and financial scams' (Fenge, 2017, p.66).

1 in every 14 of the population aged 65 years and over have Dementia.

(Alzheimer's Society 2016)

76% of people with dementia reported they had experienced difficulty in managing their finances

(Alzheimer's Society 2011).

Dementia can cause fluctuations in mental capacity and the ability to make decisions, judge risk and apply caution, which puts people with dementia at risk of responding to a scam (Fenge 2017). Research by the Alzheimer's Society (2011) found that 'people with dementia who have wealth and resources may attract those keen to exploit them through fraud or theft. At the other end of the scale, those with few assets are less likely to make future plans; as their cognitive abilities decline, they may find themselves struggling to manage their finances' (Alzheimer's Society, 2011, p.V).

The methods of financial transactions and management are rapidly changing, including increasing amounts of online transactions, cash machines, telephone banking and reduction in the use of cheques. This can make it more difficult for people with dementia to manage their own finances and for them to require support (Alzheimer's Society 2011).

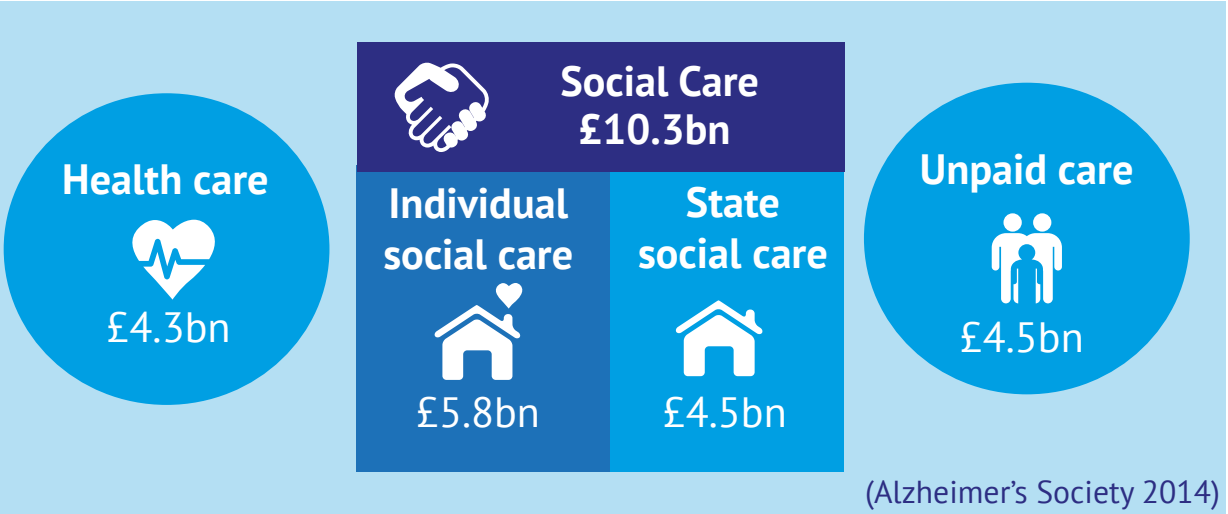
70% of carers said that nuisance telephone cold callers routinely targeted the person they cared for.

(Alzheimer's Society 2011)

Impact of dementia

£26.3 Billion per year

£32,250 per person



(Alzheimer's Society 2014)

Clear communication with those with dementia and their carers is essential in increasing awareness of potential financial scams (Fenge 2017).

NHS guidance on communicating with people with dementia offers the following advice:

- Speak clearly and slowly, using short sentences
- Encouraging them to join in conversations with others
- Make eye contact with the person when they're talking
- Encourage them to speak for themselves
- Allow time for the individual to respond
- Giving individuals simple choices – avoid creating complicated choices
- Explore other ways to communicate – such as rephrasing questions because they can't answer in the way they used to
- Acknowledge what they have said, even if they don't answer your question, or what they say seems out of context – show that you've heard them and encourage them to say more about their answer

NHS Guide 'Communicating with people with dementia'

62% of carers said the person they care for had been approached by cold callers, or doorstep sales people.

(Alzheimer's Society 2011)

Case Study

Mr. K, 86, lost his wife 22 years ago and he now lives alone. He has health and mobility issues and does not leave his property. He is in the early stages of dementia. Mr. K replied to lottery, clairvoyant and inheritance scams. He wanted to pay for improved accommodation in a residential care home. He received 80 -120 scam letters and 20 scam phone calls a week. Mr. K has spent at least £30,000 on scams in three years, although this is likely to be much higher. With no savings, Mr. K survives on his state pension and benefits. He has moments where he understands that he has been replying to scams, but he quickly forgets.

Case study provided by the National Trading Standards Scams Team.

The Mental Capacity Act 2005

The Mental Capacity Act is a statutory framework that allows for decision making on behalf of people over the age of 16 who have a mental incapacity. The Act covers personal welfare decisions, mental healthcare decisions and financial decisions.

It has 5 principles:

1. It must be assumed that a person has capacity unless proved otherwise.
2. All practicable steps must be taken to help a person make a decision before it is deemed they are unable.
3. People are able to make unwise decisions without being deemed as incapable of making a decision.
4. Any decision or action taken on behalf of another must be done so in their best interest.
5. Before decisions are made or actions taken on behalf of another, consideration must be given to alternative and less restrictive ways of doing so.

Section 3 of the Mental Capacity Act 2005 sets out the two-stage process by which an individual's mental capacity is assessed (an assessment of capacity is both time and decision specific):

Stage 1 considers whether the person has an impairment or disturbance in the functioning of their brain or mind. The impairment may be permanent or temporary.

Stage 2 asks whether the impairment or disturbance means they are unable to make the specific decision. To clarify this, the assessor will check whether the person is able to:

- Understand information relevant to the decision
- Retain the information
- Use or weigh that information as part of the decision-making process, or
- Communicate the decision by whatever means necessary (adapted from Lyne 2017, p.86).

The term 'next of kin' has no legal authority. The law does not allow for a next of kin to consent to treatment or make decisions on behalf of another person unless a relevant Lasting Power of Attorney is in place. Lasting Powers of Attorney are enabled by the Mental Capacity Act and can be arranged to cover two aspects of decision making; firstly, health and welfare decisions and, secondly, financial management.

Unwise Decisions

It should not be assumed that a person lacks mental capacity if their decisions are thought to be unwise. We all have a legal right to make an unwise decision. Distinguishing between a lack of capacity and an unwise decision can be difficult. Responding to a scam could be seen as an unwise decision unless the individual has been diagnosed with a cognitive impairment.

Lasting Power of Attorney

A lasting power of attorney allows a person to appoint someone of their choice to make decisions on their behalf should they become unable to do so. It is a legal tool which can help a person plan for their future and manage their finances and health and social care. Lasting Powers of Attorney can help protect vulnerable people from financial scamming.

What are the different types of scam?

Scammers use a wide range of techniques and methods of communication to make contact with individuals. This means many different types of scams evolve as technology develops. Scams are designed to appeal to different people in a variety of circumstances, for a range of motivational reasons. For example, an investment scam may appeal to someone with capital who is looking to invest in a business opportunity, whereas a clairvoyant scam may appeal to someone recently bereaved.

Here are some of the most common types of scams:

Lottery or prize draw scams	Correspondence informs the individual that they have won a large prize on a lottery or draw that they didn't enter. To claim the winnings, the person must send a fee to release the funds or cover taxes.
419 scams	Individuals are offered a share in a large sum of money in return for helping to transfer it out of the country. Once scammers have the bank account details they empty the accounts.
Romance scams	Criminals, using a false identity, join legitimate online dating websites or chat rooms to develop a relationship and build up trust. The relationship is exploited to extort money with victims potentially being implicated in illegal activities such as money laundering (Citizens Advice, Scotland 2014). The financial and emotional impact may be significant (Whitty 2013).
Clairvoyant scams	These target bereaved individuals and involve very personal communications offering contact with deceased loved ones. Alternatively, 'magic' products may be sold to 'ward off' evil spirits or bring good luck, or predictions of the future may be offered in return for payments.
Catalogue scams	Sell 'miracle cures', products and vitamins at bargain or inflated prices. Products either do not arrive or are of little or no value. Respondents are sometimes entered into a fictitious prize draw as an incentive to continue ordering products.
Charity scams	Scammers may create bogus charities or impersonate legitimate charities and pocket the proceeds. Approaches from scammers may be on the street, by telephone, email or at your door. Fake websites may also be used (Action Fraud 2018).
Pension scams	Pension liberation schemes target older people by offering to convert pension benefits to cash benefits. Respondents pay high fees and often face tax bills as a result of such schemes.
Investment Scams	Investment opportunities offered in products such as wine, diamonds and land. These are high loss scams with the average loss being over £32,000 (Action Fraud 2016).The products are either non-existent or of low value. Most (77%) victims of investment fraud are men with the average age of 65 (Action Fraud 2016).
Recovery Room Scams	Individuals who have already lost money to an initial investment scam are contacted again to be told that their investments can be recovered on payments of further fees or on purchase of other commodities.

Mail Scams

The post is a common means by which scammers make contact with potential victims. Some people who respond go on to receive more than a hundred scam letters a week. Despite the growth of the internet, there is no evidence to suggest there has been a reduction in mail scams. Common mail scams include: fake lottery and prize draws, clairvoyants and catalogue scams featuring 'miracle cures' or 'luxury' products.

It is estimated that prize draw scams cost the UK public £60 million per year.

(National Trading Standards 2015)

2 in 5 of all postal scams are lotteries or prize draws.

(Citizens Advice 2015)

- ✗ **Don't pay anyone in advance for a prize or cash sum.**
- ✗ **Don't send money abroad or to someone you don't know.**
- ✓ **Check for poor spelling and grammar.**
- ✓ **Ask about the Mail Preference Service. This will not prevent all scam mail or international mail.**

Case Study

Mrs. M, 92, lives alone. When Trading Standards visited her house there was little evidence of scam mail in the living room, but it transpired she had been responding to prize draw mail scams for over 10 years and had been hiding the mail. Mrs. M's estimated spend was £500 a month, amounting to a detriment of approximately £60,000. 34 bags full of scam mail were removed from her house.

Doorstep Scams

Scammers commonly pose as legitimate doorstep traders and attempt to sell goods or services that are of poor quality, unnecessary, faulty, overpriced or which do not exist. In some cases, customers are unaware of the inflated price for goods or services. Customers are often billed for services that they did not ask for or which were worth considerably less. Doorstep fraudsters put people under pressure and can appear friendly, polite and trustworthy.

- ✗ **Don't pay for any agreed goods or services up front.**
- ✗ **Don't immediately agree to any offer or service.**
- ✓ **Get all agreements for any goods or services in writing up front.**
- ✓ **Check credentials such as ID, address and telephone numbers.**

There were 17,264 reports of doorstep crime in 2014/15, but this could be as low as 1% of cases.

(National Trading Standards Board 2015)

The most prominent doorstep scams

(National Trading Standards Board 2015)

Telephone Scams

Scammers commonly make contact by telephone or text, often using a local number. They may attempt to get personal details such as PIN numbers. These scams are referred to as 'vishing'. Citizens Advice (2018) also warn of scammers using premium rate numbers. Typically, a prize is offered and can only be claimed by calling a premium rate number; callers are then tricked into staying on the line for a long time. The longer the call, the more money the scammers make. The prize never turns up or it will turn out to be an item worth less than the cost of the call.

Common telephone scams include bogus pension and investment schemes, charity scams or scammers posing as a bank official who claims that your account has been accessed by scammers and instructs you to transfer funds to a 'safe' account.

Courier scams are also common. These are usually two staged; firstly, scammers cold call, claiming to be from the bank or other authority and persuade individuals to give their PIN number. Secondly, a 'courier' picks up the card which is then used by the scammers.

Case Study

Mrs. A suffered a power cut after a storm which resulted in her telephone blocking device disengaging. During the four hours without power her daughter received 10 phone calls. After investigation, it was found that Mrs. A was receiving an average of 70 nuisance calls per month. During the worst month 121 calls were received.

58% of people received suspect calls, an increase from 41% the previous year.

(Financial Fraud Action 2014)

£23.9 million lost to vishing in one year, which is up £7 million in one year.

(Financial Fraud Action 2014)

✗ **Don't return cold calls without checking the other person is no longer on the line.**

✗ **Don't give out your PIN to anyone.**

✓ **Ask about the Telephone Preference Service.**

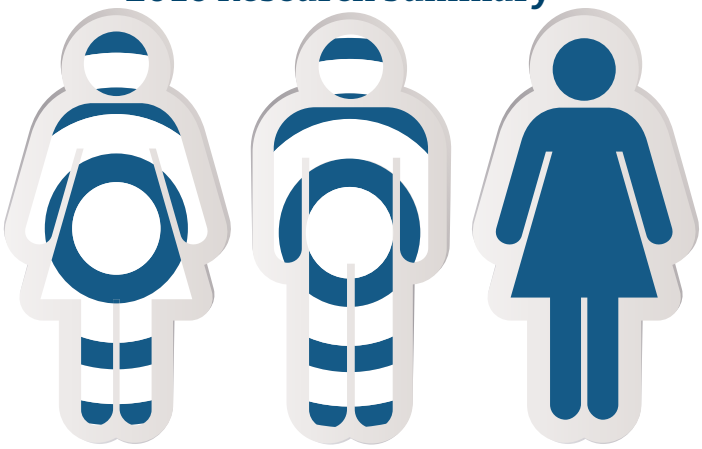
✓ **Install a call blocker.**

Cyber Scams

The internet has extended the reach of fraudsters and scammers enabling them to contact people around the world whilst retaining their anonymity.

The Crime Survey for England and Wales (ONS 2018) identified that over half of the estimated 3.2 million cases of fraud (56% or 1.8 million incidents) in the year ending September 2017 were cyber-related, with a further 1.5 million computer misuse offences. These estimated figures represent a fall in the number of incidents, which the ONS accredits to reduced online shopping fraud, fraudulent computer service calls and a fall in "computer viruses" (ONS 2018). However, the ONS counsels caution as the figures are dependent on the willingness of people to report.

Get Safe Online Survey, Action Fraud, 2016 Research summary



Over 2 out of 3 people have been targeted.
Most people do not realise that they have been targeted.

(Action Fraud 2016)

Authorised push payment scams – these are online payments authorised by the individual who has been tricked into paying a fraudster or scammer. UK Finance (2017) states that £101.2m was lost to payment scams in the first six months of 2017. Online payments are generally made through the Faster Payments Scheme, meaning scammers receive the funds immediately and account holder has no time to realise they've been scammed and cancel the payment.

Identity fraud - makes use of a stolen identity to obtain goods or services by deception; for example, open bank accounts or apply for credit cards, loans and state benefits, or obtain passports and driving licences. The person may only become aware of the scam when they receive letters from, for example, debt collectors for debts (Action Fraud 2018).

Phishing - these are emails which are sent to thousands of people at a time. They appear genuine, but are designed to get recipients to reveal personal information, click on bogus or harmful links or attachments.

Pharming and copycat websites – fraudulent websites mirror legitimate sites to deceive the users into inputting their login details or confidential information where they are then accessible to scammers. Copycat websites provide what appears to be a legitimate service but at a premium charge.

Social engineering – most of us tend to be helpful and want to be cooperative; fraudsters and scammers take advantage of this and will skilfully manipulate us to divulge personal information through, for example, impersonating a legitimate organisation such as a bank, HMRC or a government department. This sort of deception often happens online.

Romance fraud/online dating scams - fake profiles are used to contact potential targets and gain their trust. Grooming techniques are used to develop the relationship and, in time, the individual is financially exploited. Scam packs containing fake love letters, profiles, videos and false identities can be purchased on the dark web.

Payment fraud – often targets businesses and attempts to get employees to transfer money into the scammer's account by impersonating a senior member of staff.

Mandate fraud - scammers will get the account holder to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example, a subscription or membership organisation or your business supplier (Action Fraud 2018).

Pension Fraud and Pension Liberation Fraud/Scams

Pension liberation involves the transfer out of specific pension scheme benefits before retirement. Pension liberation becomes pension liberation fraud when you are not informed of the potential tax consequences involved and/or when some or all of your money is unable to be found.

Pension liberation scams see your money transferred into often high risk investment opportunities which are frequently based overseas and are not regulated by the Financial Conduct Authority. Without such regulation there is no protection should anything go wrong. These schemes often claim to allow people to access to their money before they turn 55, with the promise of "guaranteed" investment returns that are just too good to be true.

A cold call or email tempting an individual to release monies under the following guises maybe received:

- **a 'legal loophole'**
- **to 'maximise the flexibility available under the Government's new Pension Freedoms'**
- **an offer of a free pension review**

Organisations offering these opportunities frequently refer to them as 'pension loans' and offer cash incentives to sign over their pension benefits. A courier may be sent to the victim's home address with transfer documentation to sign. Many people are likely to sign the documentation whilst the courier waits rather than having the papers reviewed and seeking independent advice.

It is not legally possible for people under 55 to access the money in their pension scheme, except in rare circumstances, such as terminal illness. Whilst people do have the opportunity to transfer their pension benefits pre-retirement into another authorised pension fund, independent advice should be taken (including an actuarial calculation for transfers in excess of £30,000) to properly assess the value of the benefits held and the possible risks of transfer.

What many people also do not know is that with the illegal early access to pension assets substantial sums to HM Revenue & Customs (HMRC) will become due. Early access to pension assets is considered an unauthorised payment by HMRC. A significant additional tax charge of 55% plus interest is due on unauthorised payments and remains due even if the individual never received, or cannot recover, the liberated funds. This is irrespective as to whether a fraud can be proven. This 'double loss' can have severe ramifications rendering the individual insolvent and facing bankruptcy.

Following changes to pension rules introduced in 2015, there is now even greater flexibility available for an individual to access their pension and, in turn, an increased opportunity to become a target of a scam. Anyone over the age of 55 is normally able to withdraw 25% tax free with the rest having tax deducted at source if drawn.

Research conducted by Citizens Advice shortly after the pension freedoms were introduced in 2015 suggested four out of five savers had been contacted about their pensions over the phone since the introduction of the freedoms. **In May 2017, the Financial Times reported that more than £42m has been lost to "pension liberation fraud" since April 2014.** It is suspected that this figure could be far higher given many frauds remain unreported.

The early release of pensions and any offer to invest pension monies can see an individual being misled about risks attached to such a release or transfer and the true nature of the investment. In fact many investments whilst might not being fraudulent may still result in the loss of an entire pension pot combined with the added burden of an unforeseen tax debt due to HMRC. This can see pension pots wiped out and the individual left with no way to account for their future living needs.

There are independent advisory services who can help discuss an individual's pension requirements and should be a 'go to' for anyone concerned about a pension transfer or review.

- **Pensions Advisory Service - www.pensionsadvisoryservice.org.uk**
- **Pension Wise - www.pensionwise.gov.uk**

Advice from the Financial Conduct Authority is to always check that anyone offering advice or other financial services is FCA authorised and permitted to give advice on pensions. It is necessary to be permitted to give specific pension advice and not just be registered. Check the register at https://register.fca.org.uk

Seeking independent professional advice before making any investment and ignoring any unsolicited or cold approaches can help ensure pension pots remain out of the hands of fraudsters.

Investment Scams

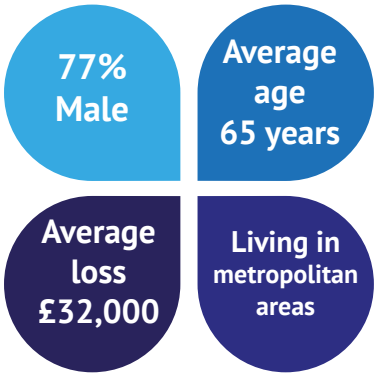
Victims of investment scams are sold overvalued or nonexistent investments with promises of high returns with low to no risk. Every year in the UK, an estimated £1.2bn is lost to investment fraud. It is generally accepted that only 10% of all crimes are reported; this means the number of people affected by investment scams is likely to be much higher.

The investments sold by the scammers are very diverse. For example, overseas holiday properties, forest land, wind turbines, rare or precious commodities such as diamonds that will only increase in value due to their scarcity. They can be sold to members of the public as part of a plan to improve a pension by direct telephone sales, or by taking advantage of less regulated investment markets. These will be schemes unregulated by the FCA. Fraudsters will also try to add credibility to their approach and they may use a firm of solicitors to give the impression of legitimacy to the investment.

If an individual is of pensionable age or in a position to invest substantial savings, they may be targeted with the use of high-pressure sales tactics or fall victim to misleading promotional statements and material. Often the fraudster builds a rapport over several weeks or months and many see the fraudster as a trusted friend before the high-pressure sales tactics are used.

Figures released in October 2016 by Action Fraud and the City of London Police show that over 77 per cent of all individuals reporting investment fraud are men with the average age of 65. Their average loss is over £32,000, with most living in metropolitan areas.

Individuals reporting investment fraud



Source: Action Fraud and City of London Police 2016

Advice from consumer bodies is to never enter into an agreement as the result of a cold call or unsolicited mail. **If an individual has lost money from a scam, they may find themselves once again a target. The scam will see an upfront fee requested, a scenario that is known as a recovery room scam.**

The Financial Conduct Authority (FCA) advises consumers to reject all unsolicited contact about investments and to check the FCA Register and Warning List before investing.

To help avoid becoming victim to an investment scam always consider the following.

1. **Has an approach to invest been made out of the blue? This is generally from a cold call.**

2. **If the offer is too good to be true, it probably is. Do not allow your want to provide for your family and future to cloud your judgment or make a hasty decision.**

3. **Verify the investment and company through external sources. This may prove difficult as many fraudsters masquerade as legitimate companies online. By always seeking specific independent and professional advice before providing any bank details or signing documentation an investment scam may be avoided. Even just speaking with a friend or family member may help raise a red flag to the investment.**

4. **Friends and family members can, however, unwittingly help others become investment scam victims. Remember, if someone you know is keen to promote an investment because they are seeing high returns they are likely to be in a scam where regular payments are made or statements sent to indicate an investment is doing well. This may be a deception to ensure individuals recruit others to the scam or, in fact, see the original person invest further monies in the misguided belief their original investment is doing well.**

5. **Never put all your savings into one investment or through the same company.**

If in any doubt about an investment opportunity always say no and report any concerns to the FCA. For more advice on how to avoid investment and pension scams please see: https://www.fca.org.uk/scamsmart/how-avoid-investment-pension-scams

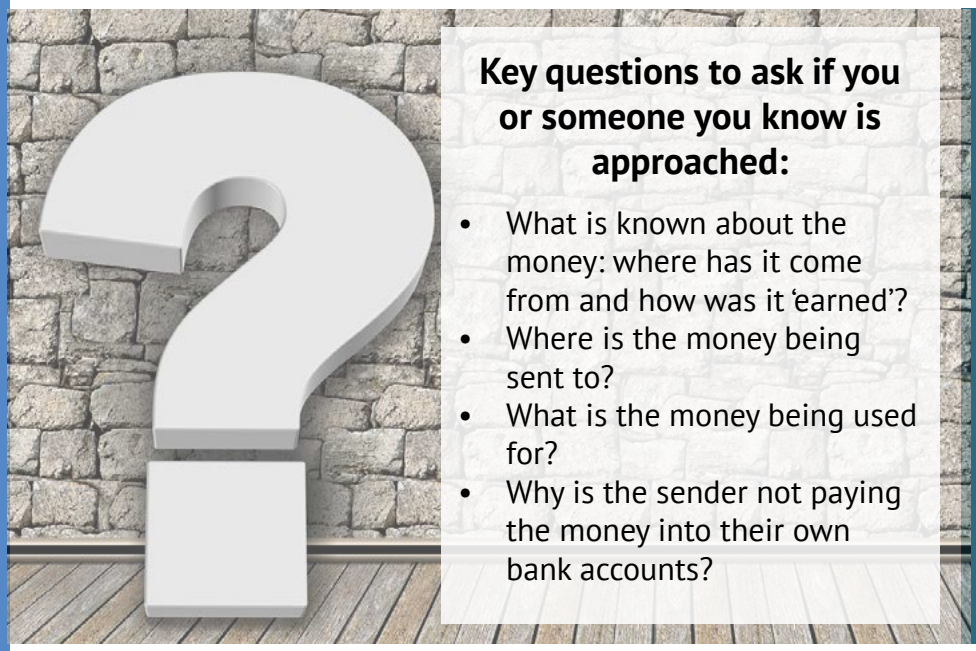
We are grateful to Samantha J Street, Associate Director, for contributing the material on Pension Fraud and Investment Scams.

Grant Thornton
An instinct for growth™

Money Mules

Criminals recruit money mules to transfer illegally obtained money between different bank accounts. Organised Crime Groups (OCG's) endeavour to set up accounts, or gain control of existing accounts, for the express purpose of moving proceeds of crime through a network of accounts in order to obscure its final recipient. The money mule's account becomes a 'Mule Account' used to launder criminal funds. The money mule will receive the stolen funds into their account, then withdraw it and transfer it to a different account (often one overseas), keeping some of the money in payment (Action Fraud 2018).

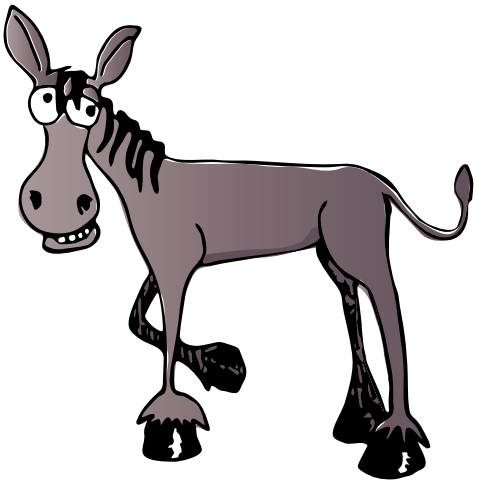
Money laundering and mule accounts are not new; however, in the UK there has been an increase in the numbers of young people allowing their bank accounts to be used to receive and move money on behalf of third parties (Cifas 2017). Young people and students are particular targets as criminals know they are often short of cash. The targets are approached and recruited through a variety of methods, for example via the internet, social media, at school, university or clubs. In some cases, they are approached by people they know and believe they can trust. They may be coerced by the offer of money or believing they are doing someone a favour.



Key questions to ask if you or someone you know is approached:

- What is known about the money: where has it come from and how was it 'earned'?
- Where is the money being sent to?
- What is the money being used for?
- Why is the sender not paying the money into their own bank accounts?

- **Never give anyone your Bank card, PIN, passcode or password – Bank accounts are private**
- **Don't be lured or persuaded to receive money into your account even as a one-off**
- **If you have been approached, break off all contact and don't receive or move any money and contact your Bank**
- **Report the matter to Action Fraud or the Police**



Potential consequences:

Criminal record - Anyone allowing criminal funds to go through their bank account is committing an offence of Money Laundering under the Proceeds of Crime Act, 2002, which carries a sentence of up to 14 years imprisonment and/or fine/community service.

Travel - Having a criminal conviction has serious implications ranging from potential employment opportunities, to travelling to other countries. Some countries, for example Canada and the USA, can refuse entry on the grounds of even minor criminal convictions.

Credit rating -Allowing a bank account to be used by an unauthorised person breaches the terms and conditions agreed between banks and their customers. Such misuse may result in the account being closed and a report being made to credit agencies, leading to a negative or poor credit rating.

Negative or poor credit ratings mean any financial transaction requiring a rating may be affected; this includes opening another bank account or applying for a loan or mortgage.

Loan Sharks

Some of the poorest members of society have very low credit scores and are, therefore, unable to take out or borrow money from a bank or building society. People in this situation, who have an urgent need for a loan to pay for a replacement fridge or cooker or to buy food, will often turn to a loan shark without realising the very serious consequences of this course of action.

As loan sharks operate illegally, their debts aren't normally enforceable in law, therefore they can only resort to other methods to enforce repayment.

STOP LOAN SHARKS
Intervention . Support . Education

If you or anyone that you know needs help then call the Hotline on 0300 555 2222.
Text: 07860022116.
Email: reportaloanshark@stoploansharks.gov.uk or find us on Facebook or visit the stop loan sharks website.

Typically loan sharks...

- **Start out being friendly - they are often heard of via friends. It is only when repayments are missed their behaviour changes.**
- **Offer little or no paperwork.**
- **Increase the debt or add additional amounts.**
- **Refuse to tell the borrower the interest rate, how much they still owe or how long they will be paying back. (We have seen APR as high as 7.2 million %).**
- **Take items as security - this may include passports, driving licences, jewellery or even bank or post office cards with the PIN to withdraw directly from borrower's accounts.**
- **Resort to intimidation, threats or violence.**

Why do people borrow from a loan shark?

- **Funerals/health costs.**
- **Christmas/celebrations.**
- **To help family members**
- **To pay off other debts.**
- **Repairs to home.**
- **Replacement of essential household items.**
- **Suspension of state benefits or awaiting benefits to be implemented.**
- **Everyday living expenses.**

The Illegal Money Lending Team has supported more than **27,500 victims** so that gives you an indication of the scale of the issue.

The England Illegal Money Lending Team is funded by the Treasury through a levy on the consumer credit industry. It works in partnership with local trading standards team across the country. They are a standalone Trading Standards units covering England that identifies, investigates and prosecutes Illegal money lenders otherwise known as loan sharks.

The Illegal Money Lending Team supports victims of loan sharks working with partner agencies to solve problems and enable people to move forward in their lives.

The team investigates and prosecutes activities related to illegal money lending, including threatening behaviour, violence, intimidation, drugs offences, kidnap and rape. A 24/7 confidential hotline for people to report illegal lending to trained investigators is available on 0300 555 2222.

The Team operate a "parachute-in" model from a centralised base in Birmingham, with up to 30 specialist investigators moving to the area once a suspected illegal lender is identified. A local presence is maintained with Leads In Awareness, Intelligence, Support and Education (LIAISE) officers in every region. These officers work in communities supporting victims, raising awareness, organising community events and initiatives and working with various partnership agencies including housing associations, credit unions, the CAB, police and debt advice services to ensure front line staff know how to spot an illegal lender in order to help their clients. Most of the awareness raising is funded using proceeds of crime money taken from convicted loan sharks.

We are grateful to the National Illegal Money Lending Team (England) Regulation and Enforcement Trading Standards for providing the material on loan sharks. Further information is available at: www.stoploansharks.co.uk.

Emerging Threats

National Trading Standards have used intelligence gathered from across all NTS work areas to identify the Top 7 rogue trading threats:

Energy saving scams	The end of the Green Deal has coincided with increasing numbers of cases involving energy-related scams dealt with by trading standards officers – many focused around nuisance calls.
Criminals selling on social media	The trend is for an increasing variety of what can be bought through Facebook, Gumtree and other sites – for example there's been a spate of 'clocked cars' (where a car's mileage is adjusted downwards to add value) being sold in this way.
Telephone preference scams	The Scams Team has seen a growing number of companies selling 'call blocking' devices that are ineffective and lead to unexpected charges. Known as telephone preference scams, the scammers cold call people claiming to be from the Telephone Preference Service (TPS) and then charge them for registration or for useless call blocking devices.
New opportunities for loan sharks	Loan sharks take advantage of those on a low income who may struggle to obtain credit via other means.
Subscription traps	Consumers or businesses are enticed to sign up to a free trial of a product or to pay a small fee to access an offer. But the offer is – intentionally or not on the part of the company – misleading and so without realising it, the respondent is then trapped into making costly monthly payments without their informed consent, which can be difficult to stop.
Investment scams	Changes to pensions that came into effect in April 2015 mean that people can access their pension money when they reach the age of 55. Criminals have been quick to create new scams such as a free pension review, where criminals contact you and offer to transfer your pension fund into a high risk investment.
Secondary ticket sales	With the explosion in secondary ticket selling platforms such as StubHub and SeatWave and more people than ever informally selling tickets through social media platforms, it has never been easier for fraudsters to pose as official dealers or genuine fans with a couple of spare tickets to sell.

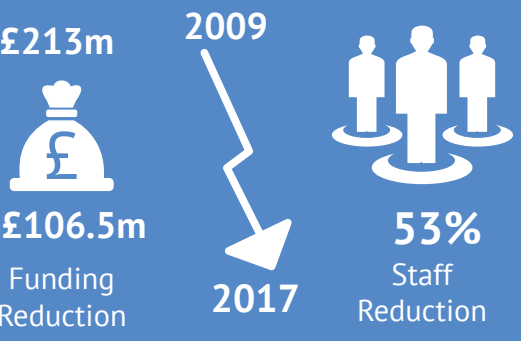
What can be done?

Enforcement

Local authorities have a duty to protect and prevent: it is a whole authority responsibility including Police, Trading Standards and Adult Social Care.

Council Trading Standards teams discharge about 250 statutory duties concerning everything from disease outbreak to product safety and rogue trading (Spicer 2014). The total GB budget for trading standards has fallen from £213m to £106.5m since 2009, resulting in a 53% cut in staff (CTSI 2017).

Total GB budget for Trading Standards



"Councils must also consider the government's enforcement priorities (their role in), the first of which focuses on consumer protection, doorstep crime, counterfeit goods and mis-selling by measurement."

Leon Livermore, CEO CTSI

Police Enforcement of doorstep crime:

There is a lack of uniformity of service delivery to vulnerable people and to offending despite 95% stating that their crime plan/PCC strategy includes protecting the vulnerable.

The Doorstep Crime Report 2015 shows that 14% of police forces gave DSC high priority, whereas it was a low priority for 32% of forces. 72% said this was due to resources, 78% said they had higher priorities, 33% lack of awareness,17% lack of training, 17% said low crime levels.

The lack of a crime code, or flag, for rogue trading/ doorstep crime incidents is currently a barrier for retrieval of incidents from crime recording databases and consequently the sharing of intelligence and the scrutiny of not just crime rates, but also the response that the crimes receive.

The report identified 32% of forces acknowledged they didn't investigate DSC to the same standard as other crimes and 62% were unable to monitor or analyse levels of DSC. That 86% of forces said the introduction of a crime code would improve their response to DSC.

Trading Standards Enforcement of Doorstep Crime

The average number of prosecutions per LA in England and Wales has remained at 1 prosecution per year (1.07 in 2013/14 and 0.95 in 2014/15).

25 LAs had taken two or more prosecutions in 2014/15 (20% of responding LAs, 15% of all LAs) (down from 32 in 2013/14).

Support from Social Care

Over the last six years local authority budgets have been cut and now 26% fewer older people get help. "No one has a full picture of what has happened to the people who are no longer entitled to publicly funded care: the human and financial costs to them and those who care for them are mounting" (Humphries et al. 2016, p.3).

National Initiatives

A number of national initiatives are recognising the scale of the problem by financial crime and financial scams.

Some of these include:

Operation Broadway

Operation Broadway is a multi-agency approach to tackling the serious issue of investment fraud. It brings together a number of partners – the City of London Corporation Trading Standards Service, National Trading Standards, the City of London Police, the Metropolitan Police, the Financial Conduct Authority, Her Majesty's Revenue and Customs and the Insolvency Service. Investment fraudsters cold call consumers in an attempt to sell "fantastic" investment opportunities in products such as wine, diamonds, rare earth metals and even car parking spaces. The sale of these products is not regulated and the products are normally over-priced, are actually a very poor investment and sometimes do not even exist. Individual consumers have been known to lose hundreds of thousands of pounds which has a devastating effect on the victims and places additional burdens on the welfare system in the future. The fraudsters like to be associated with prestigious addresses in the City to create the impression of respectability in their glossy brochures and on their websites and they use mail forwarding businesses to give the impression that they are based in the Square Mile.

Operation Broadway is an intelligence-led approach to tackling this crime and partners meet every two weeks to share intelligence and decide on deployments to addresses in the City. It also engages closely with the network of mail forwarding businesses and virtual offices that may be inadvertently facilitating this type of crime. The useful provisions of the London Local Authorities Act are rigorously enforced, making it more difficult for the fraudsters to use a seemingly respectable address. Since 2016, the scope of this work has been widened to include a number of London Boroughs and officers have been working to enforce the provisions of the legislation beyond the 'Square Mile'. While investment fraud has been traditionally targeted at consumers aged over 55 years, new trends are developing and younger people are being drawn into scams via social media. One area of concern involves binary options which are often marketed as an investment but are nothing more than a gamble on the movement in share or commodity prices. Statistics show that over £80,000 has been lost every day to binary options fraud. Operation Broadway carried out a major piece of work during 2017 into binary options and conducted visits to over 100 premises in the City. It is anticipated that the next problem with investment fraud will be related to rogue elements of the cryptocurrency sector.

Every incident of investment fraud involves the transfer of money from a vulnerable consumer to the criminal. There is, we believe, an opportunity for the financial services sector to build safeguards into the system to prevent this despicable type of financial abuse and the City Corporation will continue to engage with partners in the search for a workable solution.

Steve Playle, Trading Standards Manager for the City of London Corporation. (February 2018)

National Initiatives

Friends Against Scams

Friends Against Scams is a National Trading Standards Scams Team initiative which aims to protect and prevent people from becoming victims of scams by empowering communities to... 'Take a Stand Against Scams.'

Friends Against Scams is designed to inspire action, highlight the scale of the problem, change the perceptions of why people fall for scams and make scams a community, regional and national topic.

By attending a Friends Against Scams awareness session or completing the online learning, anyone can learn about the different types of scams and how to spot and support a victim. With increased knowledge and awareness, people can make scams part of everyday conversation with their family, friends and neighbours, which will enable them to protect themselves and others.

Anyone can be a Friend Against Scams and make a difference in their own way.

(Friends Against Scams, National Trading Standards Scam Team 2016)

Protecting young people from fraud

Research conducted at Cifas has shown that increasing numbers of young people are affected by fraud, either being targeted by online fraudsters or unwittingly engaging in fraudulent acts themselves.

Together with PSHE Association, the national body for Personal, Social, Health and Economic education, Cifas has created four Anti-Fraud Education lesson plans with accompanying resources.

- The lesson plans are targeted at 11-16 year olds and cover Key Stage 3 and 4
- These free lesson plans are available at: www.cifas.org.uk/anti-fraud-lessons

Protecting the most vulnerable from predatory fraudsters

Sadly, fraudsters can and do target vulnerable members of our society. They exploit their circumstances for financial gain by opening bank accounts, taking out loans, setting up and spending on credit cards or committing to expensive mobile phone contracts.

Cifas offers a free service for individuals subject to a Court Order of Protection under the Mental Capacity Act 2005 and who are deemed as incapable of managing their own finances.

If these vulnerable individuals' details are misused, they may be exposed to financial losses or liabilities, and potentially being labelled as a fraudster when contracts are not honoured. It can also cause them, and those caring for them, significant distress.

Our free Protecting the Vulnerable service can help prevent that distress. We work with public bodies to securely house details of their vulnerable clients in our National Fraud Database.

If one of our 400+ member organisations receives an application for a product or service in the registered person's name and they search Cifas' database, they will get an alert informing them of the individuals' vulnerable status. The application is then automatically declined, and any fraud prevented.

To find out more about Protecting the Vulnerable, please visit: www.cifas.org.uk/ptv

National Initiatives

Joint Fraud Taskforce

The new Joint Fraud Taskforce brings together banks, payment providers, police, wider law enforcement and regulators to jointly tackle this threat. It builds on the success of the Joint Money Laundering Intelligence Taskforce set up in 2015. Five workstrands are identified:

- Understanding the threat
- The collective response
- Victims and vulnerability
- Behaviour change
- Tackling systemic vulnerabilities

The development of a national taskforce is positive and to be welcomed, and will encourage greater cooperation between banks, law enforcement and government to respond to fraud. It will be important for the taskforce to consider the impact of fraud on individuals as well as businesses, and to collaborate with other agencies involved in this work including Trading Standards, The National Trading Standards Scams Team and Bournemouth University.

We believe it is important that certain groups are recognised as being at increased risk of scam involvement, and this includes older people and those who are socially isolated and living alone. In particular, those with dementia find it difficult to understand risk and apply caution to decision making due to their cognitive deficits and reduced financial capability. This makes people with dementia at increased risk of responding to scams. Therefore, banks and other financial institutions should have a 'duty to care' for those with cognitive impairments who may make an 'unwise decision' a result of their cognitive state. It is important to ensure that vulnerable citizens are protected and supported in the best way possible.

(Home Office 2016)

Call Blockers

New research by Trading Standards (East Renfrewshire Council 2016) has found that using new call blocking technology blocked up to 98% of nuisance calls. Residents reported a positive impact, leaving them feeling safer and in greater control of who contacts them.

Recommendations, which are now being investigated further by the councils who participated in the research, include:

- Installation of call blocking technology in all council sheltered housing
- The technology being made available to vulnerable adults or people involved in scams such as community alarms
- Empower residents and consumers to protect themselves through education about the risks of nuisance.

A resident, whose mother trialled the call blocking technology, said: "This has made a huge difference to my mother who has dementia and lives alone. She no longer gets anxious and agitated from PPI, insurance and cold calling calls. I cannot impress on you the positive impact this has made."

(National Trading Standards 2016)

Initiatives

Age UK: Scams Prevention and Victim Support Tool Kit

This is an interactive learning toolkit using diverse media and learning methods to inform learners about financial scams and fraud and how to support individuals involved with scams.

The toolkit provides powerpoint slides with supporting activities and information giving an in-depth learning resource for Age UK and their partners. In addition, interactive games have been developed to engage individuals and groups in activities designed to inform and raise awareness in fun ways.

The National Centre for Post-Qualifying Social Work and Professional Practice

Bournemouth University

The National Centre of Post-Qualifying Social Work and Professional Practice (NCPQSWPP) has been investigating financial abuse from scams for over three years. We work in collaboration with key partners from across the public, voluntary, financial and law enforcement sectors, including the Chartered Trading Standards Institute, National Trading Standards Scams Team, Royal Mail, the Burdett Trust for Nursing and Which? In partnership with these agencies, we are committed to developing both professional and public understanding of the risks posed by financial scams. NCPQSW leads research into scamming and publishes practice guides, literature and resources.

For further information please go to www.npqsw.com.

References

Action Fraud (2016) Cited in Operation Broadway: Innovation in Partnership – Tackling investment fraud in the City of London and beyond. [Restricted]

Action Fraud (2018) Charities. [Online] Available at: https://www.actionfraud.police.uk/charities

Age UK (2015) Only the Tip of the Iceberg: Fraud Against Older People, Age UK, London

Age UK (2014) Evidence Review: Loneliness in Later Life, Age UK, London

Alzheimer's Society (2011) Short changed: Protecting people with dementia from financial abuse, Alzheimer's Society, London

Alzheimer's Society (2014) Dementia UK: Update (Second Edition), Alzheimer's Society, London

Alzheimer's Society (2016) Demography, [ONLINE] Available at: https://www.alzheimers.org.uk/site/scripts/documents_info.php?documentID=412 [Accessed 29/01/16]

Association of Chief Trading Standards Officers (ACTSO). (2015). Doorstep crime project report 2014/15. National Tasking Group. Basildon: Essex.

Care Act (2014) [ONLINE] Available at: http://www.legislation.gov.uk/ukpga/2014/23/contents/enacted

Carter, E (2017). The language of scammers. In (eds) Fenge,L., Lee, S. and Brown, K. 2017. Safeguarding Adults, scamming and mental capacity. London: Sage. pp141-145.

Chang J (2008). An Analysis of Advance Fee Fraud on the Internet. Journal of Financial Crime, 15 (1), 77-81.

Citizens Advice, Scotland, (2014). Scammed and dangerous. Available at: https://www.cas.org.uk/publications/scammed-and-dangerous

Citizens Advice (2015) 1 in 3 cold call scams are for fraudulent financial and professional services [ONLINE] Available at https://www.citizensadvice.org.uk/about-us/how-citizens-advice-works/media/press-releases/1-in-3-cold-call-scams-are-for-fraudulent-financial-and-professional-services/ [Accessed: 18/01/16]

Citizens Advice (2018) Premium-rate prize draw scams. [online] Available at: https://www.citizensadvice.org.uk/consumer/scams/scams/common-scams/financial-and-prize-draw-scams/premium-rate-prize-draw-scams/

Day, T. (2015). Lost in the system: Locating rogue trading incidents in police statistics. Crime Prevention and Community Safety, 17, p 189–204.

Department of Work and Pensions (2017). Pensions scams: consultation. [online] Available at: https://www.gov.uk/government/consultations/pension-scams/pensions-scams-consultation#fn:3

Donaldson, R. (2003) Experiences of Older Burglary Victims [ONLINE] Available at: http://webarchive.nationalarchives.gov.uk/20110220105210/rds.homeoffice.gov.uk/rds/pdfs2/r198.pdf [Accessed 20/01/16]

Fenge, L. (2017) Dementia, safeguarding and scam involvement. In (eds) Fenge,L., Lee, S. and Brown, K. 2017. Safeguarding Adults, scamming and mental capacity. London: Sage. pp65-77

Financial Fraud Action UK (2017). Finance industry, police and trading standards unite to tackle fraud. Available at: https://www.financialfraudaction.org.uk/news/2017/12/13/finance-industry-police-and-trading-standards-unite-to-tackle-fraud/

Fischer, P., Lea, S. and Evans, K. (2013) Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam, Journal of Applied Social Psychology, 43:10, 2060-2072

Friends Against Scams (2016) Trading Standards Scam Team [ONLINE] Available at: https://www.friendsagainstscams.org.uk/

Fundraising Regulator (2016) The Fundraising Preference Service (FPS) [ONLINE] https://www.fundraisingregulator.org.uk/support-advice-for-donors/the-fundraising-preference-service/ [Accessed: 30/11/2016]

Home Office (2016) Joint Fraud Taskforce [ONLINE] Available at: https://www.gov.uk/government/groups/joint-fraud-taskforce-management-board

Humphries, R., Thorlby, R., Holder, H., Hall, P., Charles, A. (2016). Social care for older people Home truths. [online].The Kings Fund and Nuffield Trust. Available from: https://www.kingsfund.org.uk/sites/files/kf/field/field_publication_file/Social_care_older_people_Kings_Fund_Sep_2016.pdf [Accessed: 30/11/2016]

Information Commissioner's Office (2016), Mission, Vision and Goal [ONLINE] Available at: https://ico.org.uk/about-the-ico/our-information/mission-and-vision/ [Accessed: 30/11/2016]

Kang, Y. and Ridgway, N. (1996) The Importance of Consumer Market Interactions as a Form of Social Support for Elderly Consumers, Journal of Public Policy & Marketing, 15:1, 108-117

Knutson B, and Samanez-Larkin G (2014) Individual Differences in Susceptibility to Investment Fraud. Available from http://www.saveandinvest.org/sites/default/files/Individual-Differences-in-Susceptibility-to-Investment-Fraud.pdf [Accessed 09/01/16]

References

Langenderfer, J. and Shimp, T. (2001) Consumer vulnerability to scams, swindles and fraud: A new theory of visceral influences on persuasion, Journal of Psychology and Marketing, 18:7, 763-783

Lonsdale, J., Schweppenstedde, D., Strang, L., Stepanek, M., Stewart, K. (2016). National Trading Standards – Scams Team Review. [online]. The RAND Corporation Cambridge, UK. Available from: http://www.rand.org/pubs/research_reports/RR1510.html

Lubben, J., Gironda, M., Sabbath, E., Kong, J., and Johnson, C. (2015) Social Isolation Presents a Grand Challenge for Social Work, American Academy of Social Work and Social Welfare Working Paper No. 7 Available from http://aaswsw.org/wp-content/uploads/2015/03/Social-Isolation-3.24.15.pdf [Accessed 09/01/2016]

Luo, Y., Hawkley, L., Waite, L. and Cacioppo, J. (2012) Loneliness, health, and mortality in old age: A national longitudinal study, Social Science and Medicine, 74:6, 907–914

Lyne, M. (2017). Mental capacity, safeguarding and considering best interest. In (eds) Fenge, L., Lee, S. and Brown, K. 2017. Safeguarding Adults, scamming and mental capacity. London: Sage. pp 78-91

National Trading Standards (2015) Consumer Harm Report, [ONLINE] Available at: http://www.nationaltradingstandards.uk/site_assets/files/National%20Trading%20Standards%20Consumer%20Harm%20Report%202014-15.pdf

N**HS Guide 'Communicating with people with dementia,** Available from: http://www.nhs.uk/Conditions/dementia-guide/Pages/dementia-and-communication.aspx

Office of Fair Trading (2009) The psychology of scams: Provoking and committing errors of judgement University of Exeter School of Psychology, Exeter

Office of National Statistics (2015) Principal projection - UK population in age groups 2014 based

Office of National Statistics (2016). Overview of fraud statistics: year ending March 2016. [Online] Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/ crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016#how-is-fraud-defined-and-measured

Olivier, S., Burls, T., Fenge, L., Brown, K. (2015) "Winning and losing": vulnerability to mass marketing fraud, The Journal of Adult Protection, 17:6, 360 - 370

The Pensions Regulator (2015) Pension Scams: Don't Get Stung, [ONLINE] Available at: http://www.actionfraud.police.uk/sites/default/files/Pensions%20Regulator%20-%20Pension%20Professionals%20Booklet.pdf [Accessed 19/01/16]

POPPI (2015) Living Alone, [ONLINE] Available at: http://www.poppi.org.uk/index.php?pageNo=324&PHPSESSID =jlmbne15imnjge3ed4irkbue23&sc=1&loc=8640&np=1 [Accessed 26/01/2016]

University of Portsmouth (2016) Centre for Counter Fraud Studies: Annual Fraud Indicator 2016, [ONLINE] Available at: http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf [Accessed 28/10/16]

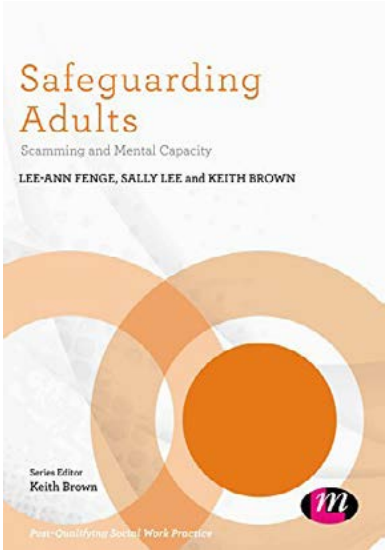
Victor, C, Scambler, S, Bowling, A & Bond, J (2005) The prevalence of, and risk factors for, loneliness in later life: a survey of older people in Great Britain, Journal of Ageing and Society, 25:6, 357-375

World Health Organisation (2016). World Health Organisation(WHO) (2016) Dementia: Fact sheet. Available from: http://www.who.int/mediacentre/factsheets/fs362/en/

Whitty, M (2013) The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology, 53(4): 665-684.

Scamming Materials Available at the NCPQSW Website

Safeguarding Adults: Scamming and Mental Capacity



This text brings together accessible information and guidance on adult safeguarding in the context of mental capacity and financial abuse. Professionals from agencies involved in scam prevention, enforcement and victim support contribute evidence and contemporary examples from practice to enable readers to understand the new landscape of safeguarding adults since the implementation of the Care Act 2014 and the introduction of Safeguarding Adult Boards. There are chapters on the current landscape of adult social work, specific issues and contexts that make people vulnerable (social isolation, mental capacity, dementia), and important methods of assessment and intervention. A range of techniques are used within the text to enhance learning including case studies, reflection points, brief exercises and further reading.

Burdett Trust for Nursing: Safeguarding practice for those at risk of financial abuse from scamming

This learning tool, funded by Burdett Trust for Nursing, supports people who have experienced, or are at risk of financial abuse from scams.

Community nurses are likely to be in daily contact with adults made vulnerable by their circumstances, and are therefore ideally located to identify and support the victims of financial abuse. Every healthcare practitioner, whatever their role, has responsibility for safeguarding the people in their care.

Although financial abuse from scamming has been a long-term social issue it is only recently that the true range, reach and impact of personal fraud on health and wellbeing has been recognised. Advances in technology have increased the opportunities for scammers to reach beyond national boundaries, but 'old tech' fraud (relying on face-to-face encounters, mail or telephone contact) remains prevalent, often targeting the lonely, socially isolated and people in vulnerable circumstances.

Financial Scamming: Defining Terms

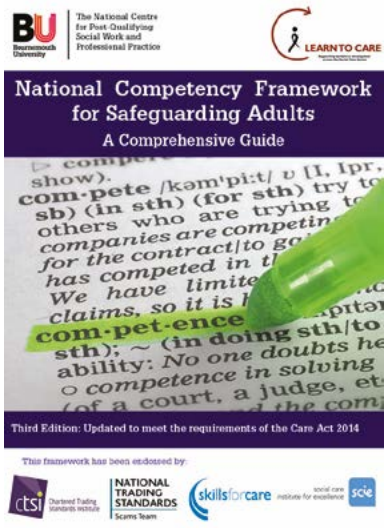
This document provides clear and concise definitions used within financial scamming and highlights the warning signs of scams.

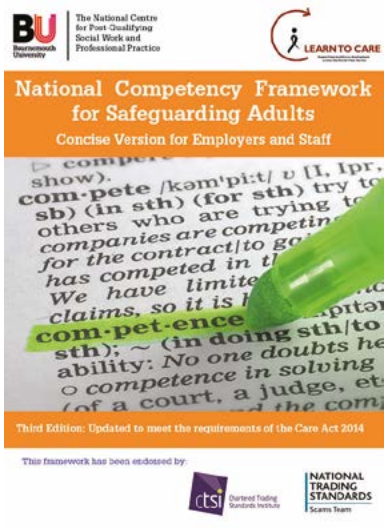
Cyber Scams: Key Facts

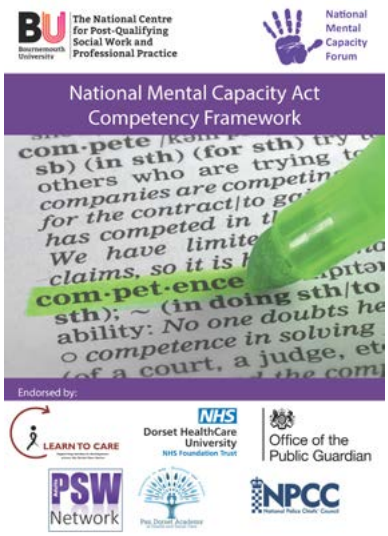
This document provides a range of definitions of words and phrases used in relation to cyber scams.

Safeguarding Adults at Risk Resources

These workbooks provide the information and training needed to establish the minimum standard of competence required of those who work with adults. The National Competency Framework for Safeguarding Adults and these workbooks, used together, enables employers and employees to establish consistency in approach to safeguarding adults.







Next of Kin: Understanding Decision Making Authorities

In law, the term Next of Kin has no status when you are alive. This helpful leaflet clarifies how people can plan, with those they love, ways to ensure their wishes are taken in to account if, through illness, they cannot make decisions for themselves.

These workbooks and frameworks enable employees to demonstrate competence in their practice in a way that is in line with their occupational role and responsibilites. For more information about publications by The National Centre for Post-Qualifying Social Work and Professional Practice, please visit our website: www.ncpqsw.com

Bournemouth University

The National Centre for Post-Qualifying Social Work and Professional Practice

Contact details

We are able to offer a single point of contact for all questions and enquiries regarding all the educational programmes we administer. Our contact details are below:

National Centre for Post-Qualifying Social Work and Professional Practice
Bournemouth University,
4th floor, Royal London House,
Christchurch Road,
Bournemouth,
BH1 3LT

Tel: +44 (0)1202 964765
Fax: +44 (0)1202 962025
Email: pqsw@bournemouth.ac.uk
Website: www.ncpqsw.com
Twitter: @researchpqsw

Lead Researcher: Dr Sally Lee
Designer: Emily Rosenorn-Lanng