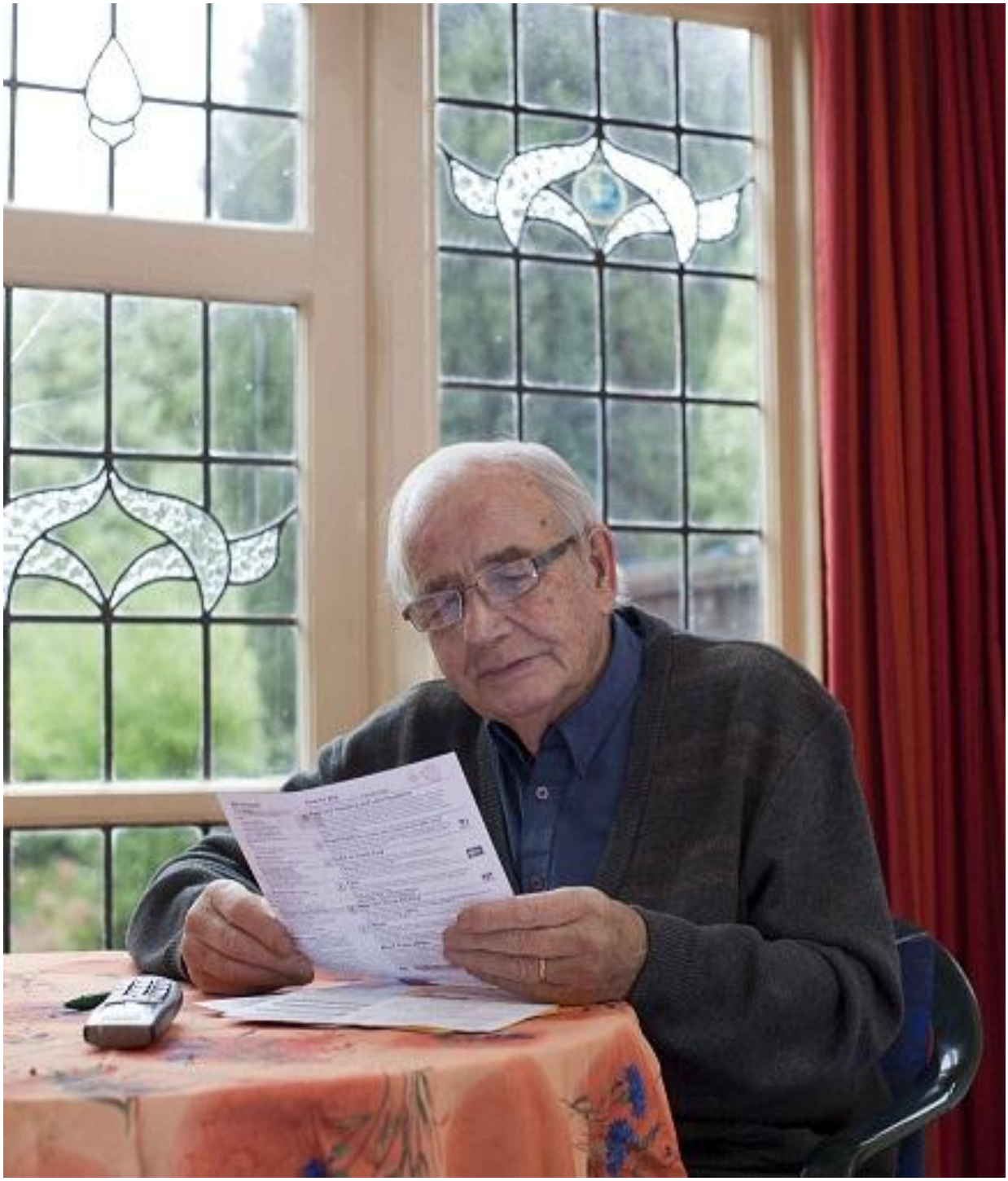
Only the tip of the iceberg: Fraud against older people

Evidence review

April 2015



We’re Age UK

Age UK is a charity and a social enterprise driven by the needs and aspirations of people in later life. Our vision is for a world where everyone can love later life.

Age UK provides information and advice to over 5 million people each year, runs public and parliamentary campaigns, provides training, and funds research exclusively focused on later life. We support and assist a network of around 165 local Age UKs throughout England; the Age UK family also includes Age Scotland, Age Cymru and Age NI. We run just over 450 Age UK charity shops throughout the UK and also offer a range of commercial products tailored to older people.

Contents

About this report

This report aims to contribute to the wide-ranging work underway to tackle fraud and 'scams'. It reviews the existing evidence of how older people in particular are affected by the full range of 'scams'. This gives us, and others working in the field, a solid evidence base to help us move forward and develop more and better solutions.

Age UK receives hundreds of queries every year from people worried that they or their family have been 'scammed'.
The words 'fraud' and 'scams' are used interchangeably in the report. We acknowledge the debate about the appropriateness of each term but have decided to use both to help us pull together the full range of evidence, data and stakeholders working in the field. We are clear that 'scams' are often sophisticated acts of deception, resulting in significant detriment and harm and about which no victim should ever feel ashamed.

The report was commissioned by Age UK and written by George & Lennard Associates: namely Mike George, Professor Cosmo Graham, University of Leicester, and Linda Lennard. We extend our thanks to them for this exhaustive and invaluable work.

They would like to thank the numerous organisations and experts contacted during the course of the research for this report who assisted us with information and advice. Any errors are of course our own.

Foreword

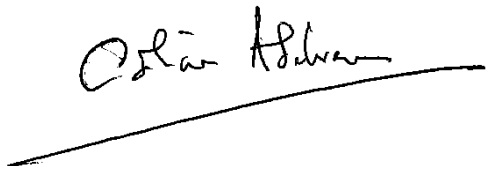
The idea that anyone would deliberately target an older person for the purposes of fraud is so abhorrent that most of us prefer never to think about it. But this report shows that we really do need to and for three reasons in particular: because older people are more likely than others to be targeted by, and so become victims of, certain scams; because scams against older people are prevalent (and under-reported); and because when it happens the consequences for older people are often severe and long-lasting.

Worryingly, there is every reason to suppose that the threat posed to older people is increasing. For example, the numbers living with dementia and cognitive decline are significant and growing and some fraudsters conscientiously search such people out in order to part them from their money. In addition, while the internet brings many wonderful things it also opens up new possibilities for fraud and as more older people go online, so the numbers potentially at risk of being defrauded also rise.

The degree of sophistication used to pull off some successful online or telephone frauds against older people is truly frightening, but so too is the brazen approach shown by the perpetrators of much more traditional forms of the offence – such as the fake doorstep tradesman who asks for money up front from a frail older person living on their own and who is never seen again.

For all these reasons and for many more made clear within the text, this comprehensive overview of what is known about fraud against older people in Britain should act as a wake-up call. There is more for all of us to do to help prevent and tackle these obnoxious crimes but for Government and other policymakers the implications are clear: scams against older people are a serious national and international problem that demands a much more determined and strategic response than it has so far received. This has to change.

And for Age UK this is just the beginning of the work we intend to do over the next year in order to give the problem of fraud against older people the attention it needs, with the aim ultimately of reducing its prevalence as well as its frequently awful impact on the older people of this country.



Caroline Abrahams
Charity Director

Executive summary

- Age UK has found that over half (53 per cent) of people aged 65+ believe they have been targeted by fraudsters.[i]
- While only one in 12 responded to the scam, 70 per cent of people of all age groups who did respond said that they had personally lost money.
- This could mean that a staggering half a million older people have fallen victim to losing savings.
- Recent reforms to private pensions make it likely that people retiring will be targeted by fraudsters who know that they can now draw all their pensions in cash.
- There is an urgent need for stronger leadership, coordination and ambition in tackling scams. Age UK calls on the Government to set up a National Scams Task Force to bring a renewed focus, building on the good work that is already going on.

We are particularly concerned that recent changes to **private pensions** will encourage scammers **to target older people**

Scams and older people

Scams are a major threat to older people's financial security and overall health and wellbeing. This report reviews the available evidence on scams and older people, highlighting the different types of scams, the factors that put some older people at risk, the impact of scams, the extent of scams and the legal context. It does not cover financial abuse carried out by someone known to the victim, such as a relative, neighbour or carer; this is an important topic that deserves a report of its own.

Scams, or frauds against individuals, take many forms. As well as scams carried out on people's doorsteps, the opportunities for fraud have massively expanded in recent years. Fraudsters can now target very large numbers of people from the UK and overseas by online methods, through the mail and by phone calls and texts. Tactics include befriending and 'grooming', the use of seemingly professional documentation and websites, impersonating a bank or the police, and threats or intimidation.

Anyone can become a victim of scams, including people of all ages and those who are financially sophisticated and confident. But within this diversity of victims, older people may be particularly targeted, often because it is assumed that they have more money than younger people. Age UK is particularly concerned that recent changes to private pensions allowing people aged 55+ to take all their pension savings in cash will encourage the scammers to target this age group even more.

And while people of all ages are targets, it is clear that older people are at special risk of certain types of scam such as doorstep crime, bank and card account takeover, pension liberation scams and investment fraud. While younger people may be more likely to be at risk of online fraud, increasing numbers of older people are likely to be at risk as the percentage online is expected to grow.

Older people may be especially at risk of becoming a victim at particular times because of personal circumstances, such as social isolation, cognitive impairment, bereavement and financial pressures.

Older people may be especially at risk due to social isolation, cognitive impairment or bereavement

It is extremely worrying that people in vulnerable circumstances may be put on so-called 'suckers lists' that are used and shared by fraudsters in the UK and overseas. This can lead to people being repeatedly targeted; for example, being sent many letters every day. This can result in people becoming 'chronic victims'.

While the effects of being a victim vary, the consequences can be highly damaging and long-lasting for the person's physical and mental health, relationships and finances. Some victims lose tens of thousands of pounds from hard-earned savings. People's health can spiral downwards following a scam. Those on a fixed income and/or who have long-term health problems may find it especially difficult to 'bounce back' financially and in terms of health.

It is very difficult to get an accurate picture of the prevalence of scams, due to under-reporting and difficulties in measuring fraud incidents. A 2013 estimate by the former National Fraud Authority put total losses for individuals at over £9 billion per annum. This is a useful indicator but is likely to be a significant under-estimate due to under-reporting and the fact that it may not include every type of fraud.

Recent research by Age UK found that 53 per cent of people aged 65+ believe they've been targeted by fraudsters. While only one in 12 responded to the scam, 70 per cent of people of all age groups who did respond said they had personally lost money. This could mean that a staggering half a million older people have fallen victim to losing savings. What is more, the research also suggests that a third of older people who responded may have lost £1,000 or more.

A renewed focus at a time of risk

Despite the valuable work already underway to tackle scams by central and local government, especially Trading Standards, the police and other agencies, there is an urgent need for stronger leadership, co-ordination and ambition. The growing number of older people in our society, coupled with the new access to large saving pots under the pension reforms and the fact that more older people are going online, means that tackling every type of scam has to be a priority.

Age UK calls on the next government to establish a National Scams Task Force to bring a renewed focus to tackling scams, to co-ordinate the various activity and agencies so they are more effective, and to report annually on progress and risks.

01

Introduction

The focus of this research is on fraud in relation to individual consumers, particularly older people. (Financial abuse committed by close contacts such as relatives and care staff was outside the remit of this work.)

The aim of the review was to explore the evidence base regarding the prevalence of fraud against consumers, including older people; the range of different types of fraud; who is being targeted and how; the impact on victims; and the legal and statutory framework. This evidence is invaluable as Age UK continues to work on this issue and develop policy recommendations.

This review highlights key gaps in current information and research. The most striking gap that has emerged relates to the absence of a sound and comprehensive UK evidence base on the prevalence of fraud against individuals. Similarly, there is a worrying lack of an up-to-date evidence base regarding the experiences and circumstances of fraud victims, including older people.

As a result, carrying out an evidence review has been a complicated task and it is not easy to ascertain the extent to which older people are being affected by fraud and in what ways. However, it is clear that many older people are at risk of being targeted by certain types of fraud and it is a matter of serious concern that some older people in vulnerable circumstances are being targeted, often repeatedly. Furthermore, as more older people go online, more are likely to be at risk of online fraud.

These findings have been drawn from a wide-ranging review of published material, together with additional information from a number of organisations and academic experts. Due to time constraints it was not possible to review evidence from other countries.

It is clear that many **older people** are at risk of **being targeted** by certain types of fraud

02

Types of fraud and who is at risk

Fraud or scams are not a new phenomenon. There is now a wide and seemingly ever-expanding spectrum of activities that are targeted at defrauding individual consumers.

Research by the University of Exeter in 2009 showed that up to 20 per cent of the UK population could be particularly vulnerable to scams, with previous victims consistently more likely to show interest in responding again. Moreover, good background knowledge of the subject matter (such as experience of investments) may actually increase someone's risk of becoming a victim through 'over-confidence'.[1]

The reality is that anyone can become a victim.[2] For example, research findings have pointed to the diversity of fraud victims and shown that 'greediness' and 'stupidity' were not the main factors in whether people became victims of fraud.[3]

Fraud and older people

Determining who is at most risk of fraud is not a straightforward matter. Evidence about the extent of fraud and characteristics of victims is patchy. Moreover, research has shown that it is important to distinguish between who the fraudsters are targeting, who succumbs and the actual number of victims across different demographic groups.[4]

Anyone can become a victim but certain consumers are targeted by specific types of fraud

There is general agreement about the very high levels of under-reporting of fraud by individual victims, which makes it very difficult to obtain an accurate picture. However, from the available literature and anecdotal evidence, it is clear that certain consumers are targeted by specific types of fraud. For instance, criminals may assume that older people are more likely to be at home during the day and therefore more likely to be susceptible to doorstep crime. Younger people may be more targeted by online fraud on the assumption that older people are less likely to use the internet, although this may not be the case in future as more older people go online.

Survey findings for the former National Fraud Authority (NFA) showed that victims of fraud are diverse, including those who are young, educated and

professional through to people who are older and more vulnerable.[5] The complexity of the issue was underlined by OFT research in 2006 on mass marketed scams, which found that, while older consumers were more likely to be targeted (over 55s accounting for almost half of people claiming to have been targeted), there was no evidence to suggest that older people were more likely to be victims.[6] The OFT suggested that this could partly be a reflection of greater reluctance among older victims to admit to being scammed.

The financial loss for older victims was nearly twice as much per scam as for younger victims

However, it is important to note that the financial loss for older victims (those aged 55 and over) was likely to be nearly twice as much per scam as that for younger age groups.[7] Also, it may be surmised that, for many older people on a fixed income (and no easy means of building new savings for example), it is likely to be more difficult for them to replace money that is lost as a result of fraud than for people of working age. Nearly half (49 per cent) of all people aged 75 and over live alone; and 17 per cent of older people have less than weekly contact with family, friends and neighbours.[8] People who are more socially isolated may well be more vulnerable to fraud, for instance, if they have little chance to discuss matters with others.

Contact methods and techniques

Fraudsters use a wide range of methods to contact potential victims. Consumers may be faced with fraudsters calling at their homes, letters, telephone calls, as well as using online methods.

Tactics used often include befriending or 'grooming' potential victims as well as threats and intimidation. Fraudsters may also seek to exploit people's trust of authority by making a fraud appear to be a legitimate offer from a reputable business or official institution, according to research by the University of Exeter and the OFT.[9]

Fraudsters use a variety of ways to identify potential victims, including obtaining information about people from openly available directories and databases or from marketing lists, according to findings by the Centre for Counter Fraud Studies at the University of Portsmouth.[10] Other methods highlighted in this research included how some fraudsters target 'affinity' groups of people, for example, people who work together or are members of the same clubs, or simply use advertisements to attract potential victims.

Some people who have been victims of fraud may be targeted repeatedly, and may end up on so-called 'suckers lists' as people who are likely to be vulnerable to a scam.[11] People whose details are on these lists can receive multiple letters per day. Some may be put on a 'suckers' list after only replying to a scam letter for the first time. Such lists may be used by fraudsters in the UK and/or sold on to those in other countries.

Fraud techniques

Research findings identified a range of core techniques used by fraudsters:[12]

- **Use of appropriate and latest technology**, particularly the use of the internet.
- **Professional** and **legitimate** appearance of information.
- **Illegitimate appearance**, where the involvement in an illegal activity, such as money laundering, makes it more difficult for the victim to report the fraud.
- **Small sums of money**, which make it less likely the victim will report the fraud.
- Clever **sales techniques**.
- **Selling a dream**, where the fraudster offers something someone wants at a low price or something that promises to make above average returns.
- **Operating in a legal hinterland**, where the tactics used make it difficult to unambiguously identify it as fraud.
- **Intimidation** and **threats** of violence.
- **Identity fraud techniques**, where the fraudster acquires either genuine identity documents, such as a passport or driver's licence, credit card or specific personal information.
- **Pretext calling**, where fraudsters pretend to be someone they are not to secure bank account and other personal data. It may be done in person, on the telephone or most commonly through email.

Suckers lists

In March 2014, trading standards officers at East Sussex County Council were given a 'suckers list' of over 100,000 potential victims across the UK, following a Met police raid. The National Trading Standards Scams Team was consequently set up (it works in partnership with local authorities in scam detection, prevention, enforcement and education).

The majority of people on the list were older or vulnerable, according to one local authority. This council has been looking into a number of cases where consumers have been targeted multiple times by a wide range of fraud schemes.[13]

Psychology of fraud

There is a limited evidence base on the factors that are likely to place people at greater risk of becoming fraud victims.

Some interesting findings emerged from research in 2008/09 that looked at why some people fall victims to scams.[14] This included a review of previous literature on the subject that identified the following as plausible factors:

- **Deterioration of decision making because of high motivation**: such as large sums of money or cures for diseases.
- **Trust**: induced for example by professional or official looking documentation, apparently trustworthy communications and messages.

- **Social influence techniques**: apparent similarity, reciprocation, commitment, and consistency. People may keep sending money to the same fraudster to be consistent: they may feel they need to spend just a little bit more to finally obtain value for what they have paid out.
- **Scarcity and urgency**: perceived scarcity can enhance the subjective value of an offer - scam messages frequently emphasise the urgency or uniqueness of the opportunity offered.

As the authors noted, although all the above provide plausible accounts of scam compliance, their relevance had not been subjected to systematic empirical tests. Consequently research was carried out to provide more empirical information about the psychological processes involved in compliance, which examined differences between the responses of people who, according to their self-reports, had or had not complied with scam appeals in the past.

Victims' response to high-value incentives, reliance on signs of authority and their self-confidence were key

The principal differences that emerged between respondents who did and did not report past compliance with scams were in their response to very high-value incentives, their reliance on signs of official authority, and their self-confidence. The research findings included the following:

- **Trust**: although dependence on cues of trust and authority emerged as a significant predictor of scam compliance in the questionnaire investigation, the researchers concluded that this factor requires further investigation.
- **Social influence techniques**: the research found no evidence that scam victims are more susceptible to such techniques than anyone else.
- **Scarcity and urgency**: preliminary analysis found no evidence that they have any differential effect on victims and non-victims.
- **Self-confidence**: a measure of self-confidence and self-reliance emerged as a contributory factor to being a victim of a scam, and the authors suggested that excessive confidence in one's own judgments may play a part in scam compliance.

These findings shed some light on the factors involved in the potential factors that may cause some people to be particularly vulnerable to fraud at certain times but they also underline the need for further systematic investigation.

It is worth noting that the authors also concluded that:

> *'The decision-making processes that we have identified as underlying scam compliance are part of everyday economic decision making. It is not normally dysfunctional to be highly motivated by very large incentives, to pay attention to symbols of authority, or to have a certain confidence in one's own judgment. Scammers, we argue, seek to exploit such everyday heuristics.'* [15]

Doorstep crime

Doorstep crime covers a range of fraudulent activities such as charging extortionate prices and/or charging for unnecessary goods or services. In some cases, the visit to the person's home may be preceded by a telephone cold call or the person may have responded to a flyer received at their home.

Tactics used in doorstep crime can involve befriending and persuasion as well as pressure and aggression. For instance, analysis of victim impact reports by the National Trading Standards National Tasking Group in England and Wales found that 48 per cent of victims said they felt the offenders were trustworthy; nearly two-thirds said they were friendly; and 58 per cent said they were polite. However, nearly half of those surveyed said they felt pressurised.[16]

Building and gardening scams

Four members of the same family who swindled two older people with dementia out of tens of thousands of pounds were sent to prison following a major investigation by North Yorkshire County Council's trading standards team.

In one case, an 84 year-old widow was charged well in excess of £6,000 for a botched building repair which, even if it had been carried out competently, was valued at just £30.

An 88-year-old widower was defrauded of at least £72,000 for 'building and gardening' work but no evidence could be found of any work at all having been carried out.[17]

Who is at risk?

This type of crime appears to be particularly targeted at older and/or vulnerable adults, and can include repeat offending over time. For example, research by Citizens Advice Scotland[18] found that many victims of doorstep crime are targeted because they live alone and feel they have no one to speak to about the work before agreeing to it. This research also highlighted how people who are recently bereaved may feel out of control of issues that were previously dealt with by their partner.

Doorstep crime appears to be targeted at older people

According to analyses of victim impact surveys by the National Trading Standards National Tasking Group in England and Wales[19] (with newly identified victims since January 2014):

- 85 per cent of victims were aged 65+, 59 per cent were 75+, and 18 per cent were aged 80 to 84.
- 62 per cent lived alone.
- 63 per cent had a physical impairment, 43 per cent a sensory impairment, 15 per cent a mental health condition, 14 per cent a cognitive impairment, and 35 per cent had a long standing illness.
- 24 per cent had concerns about their memory, or their family or carers had such concerns.
- 33 per cent had experienced bereavement in the past two years.
- 36 per cent had experienced depression in the past six months.
- 37 per cent missed having people around and 40 per cent were lonely.
- 9 per cent were known to be repeat victims.

National Consumer Week

Doorstep crime was highlighted in National Consumer Week in November 2014 through the 'Good neighbours stop rogue traders' campaign, a partnership led by the Trading Standards Institute (TSI), Citizens Advice and the National Trading Standards Board.[20]

Nominated neighbours give older or vulnerable members of the community a postcard for their door with the nominated neighbour's address and phone number, informing cold-calling doorstep traders to speak with the nominated neighbour on the resident's behalf. This prevents direct contact between the vulnerable resident and the trader, reducing the risk of doorstep crime taking place.

Other material included a training pack produced by Citizens Advice on how to recognise potential doorstep crime and how to get help.

Mass marketing fraud

Mass marketing fraud involves unsolicited contact by email, letter, phone or adverts, with the intention to defraud, for example, through false promises of cash prizes, or goods or services in exchange for upfront fees.[21]

Fraudsters may use commercially available data to tailor the first contact to the person's interests and circumstances, for instance, by identifying their age, gender, marital status, home ownership and house type, annual income, shopping habits, investments (including pensions), interests, technology usage, car ownership, credit status and health problems. This information can then be cross referenced to life events such as recent bereavement.[22]

Recent findings on online fraud[23] identified the following as among the tactics used by fraudsters:

- **Diversity of frauds**: each scam may be tailored to a particular type of victim.
- **Small amounts of money and mass targeting**: often involving smaller sums of money but it means many more people can be targeted more frequently.
- **Authority and legitimacy**: for instance, having a professional-looking website and making reference to well-known legitimate companies.
- **Visceral appeals**: appeals to needs and emotions such as financial gain.
- **Embarrassing frauds**: involving romance for instance.
- **Pressure and coercion**: for example, use of threats, time pressures, bombardment of the victim, and implications that the activity was not legal to prevent them from reporting the fraud.
- **Grooming**: for instance, the fraud starts with smaller, less noticeable amounts before escalating. Romance fraud may involve sending gifts to the victim.
- **Fraud at a distance**: distance presents challenges for many victims to confront and/or contact the

offender, and the offender may be less likely to feel empathy for the victim. Use of the internet may make enforcement intervention less likely and this may also act as a deterrent to report or for the report to be accepted by law enforcement agencies.

Who is at risk?

As with other types of fraud, up-to-date research evidence of victims of mass marketing fraud in the UK is very limited. For example, according to a recent article on online frauds:

> *'There has been a paucity of research over why victims fall for scams based on contact with actual victims, and victims of fraud in general have been neglected by researchers in comparison with other crime victims*.'[24]

From the evidence that is available, postal fraud appears to be frequently targeted at older people. According to the Trading Standards Institute and ThinkJessica, people who are older, slightly confused and forgetful are likely to be targeted and become 'chronic' scam mail victims.[25] OFT research in 2006 found that chronic scam victims are typically older, socially isolated and/or in declining mental health.[26]

Older people are particularly vulnerable to becoming **chronic scam victims**

According to ThinkJessica:

> *'Chronic victims refuse to believe they are being scammed and spend most of their time reading, sorting and replying to scams. The scam mail knits together and forms a delusional world that becomes a victim's reality. This type of victim will shun all help and advice. Sometimes clairvoyant scammers turn the victim against their families.'* [27]

Family members often feel frustrated and powerless to help their relative

Research carried out in 2009 for the former National Fraud Authority (NFA) found that older people were among those who are particularly vulnerable to becoming chronic scam victims.[28] The findings also highlighted the frustration often experienced by family members who felt powerless to help their relative. However, the scope of this research was limited: as the authors pointed out, the nature of the composition of the victim lists meant that there was a bias towards certain types of fraud victims: investment fraud, boiler room fraud and identity fraud, with mass marketing fraud being under-represented.[29]

Account takeover and courier fraud

Tactics to carry out account takeover include use of emails ('phishing'), phone or text messages pretending to be from a bank that ask the person to verify information such as passwords, PIN, account or card details. Victims may be told that the details are needed for a refund, security upgrade, or even as a fraud alert. Or someone's card details may be obtained by copying, or 'skimming', information from the magnetic strip of a debit or credit card at a cash machine or in a shop.[30]

Older people are especially at risk of account takeover

Other tactics involve fake bank websites.[31] The card details may then be used to carry out fraudulent purchases online, by phone or by mail order (also known as 'card-not-present' fraud). In some instances, the person may be tricked into making a fraudulent money transfer themselves.

With courier fraud, the victim is contacted by a fraudster alleging they are from their bank or the police, and that the person's credit or debit card needs to be collected and replaced, for example because of fraud on their account. The fraudster may claim that the call is genuine by telling the person to hang up and call the bank or police for confirmation of their identity. But the fraudster stays on the open line, and the victim may wrongly believe that they are speaking to their bank or the police. A courier is then sent to collect the card, which is then delivered to the fraudster along with the person's PIN number.

Number spoofing

'Criminals are using a new scam to make the people they are phoning believe they are speaking to a trusted organisation – like a bank – by fooling their phones into displaying any number the fraudster chooses.

The scam, known as 'number spoofing', works by fraudsters cloning the telephone number of the organisation they want to impersonate and then making it appear on the victim's caller ID display when they telephone them. The criminal will then gain the person's trust by drawing their attention to the number, claiming that this is proof of their identity, before trying to defraud them.

The advice to beat the scam is simple – never assume that someone is who they say they are just because their number matches that of an organisation you know.' [32]

(Financial Fraud Action UK scam alert)

Who is at risk?

Older people appear to be especially at risk of fraud involving account takeover: the proportion of victims of account takeover in the higher age categories has increased substantially, according to Cifas, a membership body that facilitates the sharing of information on fraud cases between organisations.[33] Plastic card and bank account takeovers have increased, and Cifas surmises that older age groups were possibly a favoured target as they were more likely to have a higher credit limit, as well as potentially being less likely to check their balance online between statements.

Investment fraud

Detailed evidence about investment fraud is now available as a result of research published recently by the Financial Conduct Authority (FCA). As with other types of fraudsters, those attempting investment fraud use a range of tactics that are often geared to the personal circumstances of the potential victim.

For instance, qualitative research for the FCA found that investment fraud victims are often approached at a point when there is a particular interplay between their financial situation, family circumstances and psychological state that provided the conditions whereby their decision to invest was made.[34] Fraudsters also attempt to mislead people with the appearance of professionalism, such as high quality documentation and well-presented sales people, according to the FCA research.

As with other types of fraud, 'grooming' or befriending plays an important part in investment fraud and it is often tailored to victims' personalities and the contexts of their lives. It may involve building friendship and trust, flattery, making victims feel indebted to them, as well seeking to isolate victims from their own networks, according to this research for the FCA. Other tactics involve use of products that appear topical and interesting.

Another interesting finding is that, the more financially sophisticated a person is, the more likely they are to become a victim of investment fraud, highlighting the sophistication of fraudsters' techniques.[35] Findings from quantitative research for the FCA on investment fraud published at the same time also concluded that it is not possible to protect yourself against investment fraud simply by educating yourself on financial matters:

> *'Discerning a fraud from a legitimate investment opportunity is not a simple process.'* [36]

Who is at risk?

Victims of investment fraud tend to be wealthy, financially sophisticated males with an escalating correlation to older ages, according to the above research for the FCA.[37] However, it is a complex picture as this research also identified over-representation among victims of people on incomes as low as £10,000 to £14,999 per annum, and high vulnerability to fraud recovery fraud (when fraud victims are told the money they have lost can be recovered) of women and of those who are retired with low incomes who often live alone.[ii]

Financially sophisticated people are **more likely** to be a victim of **investment fraud**

Pension fraud

As of April 2015, many people can take out all their pension savings in cash once they reach the age of 55. In this context, scammers are targeting savers with promises of one-off investments, pension loans or upfront cash. Even before this major reform, there were growing numbers of pension liberation frauds where people below 55 are deceived into cashing in their pensions early, sometimes into a false trading fund.[38] Victims of these scams will lose most, if not all, of their savings, according to the Pensions Regulator.[39] There is also concern that the new rules will increase the risk of investment and other types of fraud. People may be targeted through websites, mass texting or cold calls.

Who is at risk?

People aged under 55 may be wrongly told by fraudsters that they can unlock their pension early. And there are growing fears that people over 55 will also be the target of fraudsters. Steve Hyndman, head of financial crime prevention at the Phoenix Group, was quoted before April as stating that:

> '*Taking money from the over-55s who will be able, legitimately, to do what they like with their pensions pot, will be far easier than current liberation frauds.'* [40]

In the same article, Alan Higham, retirement director at Fidelity Worldwide Investments said that:

> *'The new pensions freedom has given a massive turbo-boost to fraudsters… These are often from set-ups with names confusingly similar to those of regulators and regulated organisations.'* [41]

The government has launched a free 'Pensionwise' guidance service. It is underpinned by legislation, including a provision which makes imitation of the guidance service a criminal offence.[42]

The FCA has launched a 'ScamSmart' campaign to alert people to the risks, and the Association of British Insurers, the Pensions Regulator and the Pensions Advisory Service also run various campaigns.

There are **growing fears** that **people over 55** will be the **target of fraudsters**, following **pension reforms**

03

The impact of fraud and why it goes unreported

Impact on victims

According to the former National Fraud Authority (NFA):

> *'As well as the fraud risks faced by organisations, fraud is suffered everyday by individuals in the UK. Often the impact is devastating, both financially and emotionally.'* [43]

Up-to-date research evidence on the effects of fraud for individual victims is patchy. Past research has included a large-scale survey for the OFT in 2006[44] on the impact of mass marketed scams on UK consumers.[iii] Some years later, the former NFA commissioned a series of large-scale research surveys in 2009 that included findings on victims' needs and experiences.[45] Since the NFA was abolished, it does not appear that research about fraud victims is being gathered and analysed in a comprehensive way on a comparable scale.

Similarly, there are concerns about the need for co-ordination by official bodies in tackling fraud:

> '*The UK as a whole has yet to embrace fully the idea of a collaborative, joined up, non competitive, cross sector counter fraud strategy'*.[46]

Financial impacts

It is impossible to identify a reliable and up-to-date figure of the financial losses experienced by individual consumers in the UK as a result of fraud on the basis of existing data.

Estimates of total financial losses used to be produced annually by the former National Fraud Authority up to 2013, when the NFA estimated that fraud against individuals in the UK equated to a loss of over £9 billion per annum. This figure consisted of:

- **Mass marketing fraud**: £3.5 billion
- **Identity fraud**: £3.3 billion
- **Online ticket fraud**: £1.5 billion
- **Private rental property fraud**: £755 million[iv]
- **Pre-payment meter fraud**: £2.7 million[v]

However, while these figures are useful indicators, they are likely to significantly under-estimate the scale of financial loss experienced by individuals as it does not appear that they included all types of fraud and, as indicated, many fraud offences go unreported.

Confusingly, the figure of £3.5 billion is also frequently referred to as an estimate of total financial losses

experienced by UK consumers as a result of fraud or scams. This appears to be based on estimates published by the OFT back in 2006.[47] However, the OFT estimates seem to have been based on different categories to those set out by the NFA as above. The OFT figure included the following:

- **Bogus holiday club scams**: £1.17 billion
- **High risk investment scams**: £490 million
- **Pyramid and chain letter scams**: £420 million
- **Foreign lottery scams**: £260 million

The OFT research estimated that the mean amount lost per scam was higher for older consumers (for those aged 55+, it was about £1,261) than for younger age groups (£684). Anecdotal evidence suggested that this could be the result of older victims being on 'suckers lists' and being repeatedly targeted by scammers.[48]

The mean **amount lost** per scam is **higher** for **older consumers**

With regard to the financial impact for individuals, there are some research findings pointing out that the effects vary according to people's individual circumstances. For example, according to research by the Centre for Counter Fraud Studies at the University of Portsmouth, for some people loss of a small sum of money was quite devastating, but for others, substantial sums were not considered significant. However, for most of the participants in this research, the impact was great whatever the loss.[49]

Many older people are on fixed incomes and so less able to recover from a financial loss

It should also be noted that a significant proportion of older people are on fixed incomes and may therefore be less able than younger people to recover from a significant financial loss as a result of fraud.

Other impacts

In general, the other effects of fraud for victims may vary depending on people's individual circumstances and their existing resources and capabilities, but the severity of the potential impact should never be under-estimated. The psychological effects can be severe and debilitating, including stress, anger, loss of self-esteem, shame and upset. For example, a study into the impact of doorstep crime on older victims by Greater Manchester Police showed that their health declines faster than non-victims of a similar age.[50]

Research by the Centre for Counter Fraud Studies at the University of Portsmouth identified a range of physical and/or psychological effects on people's lives as a result of fraud. Some experienced severe physical and/or mental health problems, damage to relationships, and fear of threats or violence from fraudsters. As the research authors stated:

> *'The research highlighted the need for the criminal justice system and other bodies to give fraud victims a better deal.'* [51]

The negative impact of financial abuse, regardless of the source, can result in someone becoming in need of support from social services, having not previously required such help.[52]

A study into doorstep crime showed that victims' health declines faster than non-victims of a similar age

Analysis of the effects of doorstep crime found that:[53]

- 40 per cent of victims said it had resulted in them having **reduced confidence** generally.
- 28 per cent said it had left them feeling **down** or **depressed**.
- 46 per cent said it had caused them **financial detriment**.
- 16 per cent had **not told anyone** about the crime, and 40 per cent of these said the reason was **embarrassment**.

Impact on victims

According to the OFT:

> *'Victims are often vulnerable people who may be in financial distress or are older or socially-isolated.*
>
> *The personal impact on them and on their families is often devastating in terms of future peace of mind and health. Victims can be left with damaged self-esteem and a reduced sense of self-worth. Victims suffer stress, anxiety and depression. Lives can be ruined.'* [54]

Under-reporting

Much of the fraud that is perpetrated against consumers goes unreported and therefore does not show up in official statistics:

> *'Fraud reported to the authorities is a small proportion of the fraud detected, which in turn is a fraction of the fraud that remains out of sight.'* [55]

The OFT research in 2006 estimated that fewer than five per cent of people reported scams to the authorities:

> *'The low level of reporting makes the collation of robust information about the harm created by a specific scam difficult to determine and therefore creates difficulties in developing an effective strategic response. In addition, enforcement agencies should not determine enforcement targets purely on complaint data.'* [56]

The OFT research also found that, among interviewees who did not report scams, nearly a third of victims claimed that it was not worth taking any action. 16 per cent of victims considered it unimportant and probably not of interest to the authorities and 21 per cent of victims admitted being too embarrassed to take action.

The OFT concluded that:

> 'V*ery often a victim cannot admit to themselves that they have been the victim of a scam and does not tell anyone, even family or friends'.*[57]

The idea that fraud victims are partially to blame for either being gullible or too eager also contributes to low reporting rates.[58] For example, the research cited above for the FCA found that victims of investment fraud are highly sensitive to feeling blame from others. Also, any negative response to reporting fraud makes victims feel blamed and foolish and this may well contrast directly with the relationship they had developed with the fraudster.[59]

It is estimated that fewer than **five per cent** of people **report scams** to the authorities

Doorstep crime

Doorstep crime is an area where there is understood to be significant under-reporting. The number of reports to trading standards departments in England and Wales has been estimated as representing only 10-20 per cent of incidents that are actually taking place.[60]

The following factors have been identified as among the reasons why doorstep crime may go unreported:[61]

- Fear of repercussions from offenders or their associates.
- Fear of getting involved in the criminal justice system/process.
- Fear of loss of independence.
- Lack of mental capacity.
- Not understanding/accepting they are a victim.
- Social isolation and loneliness.
- Embarrassment /self-blame.
- Considering it is inappropriate to report.
- Believing it is futile to report.
- Not knowing who to report to.
- Generational issues.
- Wanting to ignore the incident or forget about it.

Investment fraud

The recent research for the FCA on investment fraud provides insights into victims' attitudes to reporting fraud. Less than half (44 per cent) of investment fraud victims interviewed in this research said they reported the fraud to an official organisation but 40 per cent did not know about the fraud until contacted by an official agency.[62] The remainder did not report the fraud, or very occasionally took direct action. Some victims refused to admit they had been victimised, even

when others told them. Many victims discovered the fraud through an agency such as a bank, and therefore it was automatically reported.

Other findings from the FCA research showed the following:

Victim denial: When victims who have already transferred money seek to verify the authenticity of the investment, they don't want to believe they've been defrauded and so are prejudiced towards interpreting information to mean that the fraud may be legitimate. This makes clear messaging particularly important in disrupting an ongoing fraud.

Sensitivity to blame: Victims of investment fraud are highly sensitive to blame from others. When they report the crime and receive a response that makes them feel blamed and foolish, this contrasts directly with the relationship they had developed with the fraudster. In grooming victims, fraudsters flatter them and make them feel intelligent.

Lack of response after reporting: Victims who reported a crime to the FCA described not receiving any further information about what happened with the information they gave. This lack of communication, even simply to explain why it isn't being investigated at the present time, reduces victims' confidence in the FCA and other authorities. This lack of confidence leaves victims vulnerable to fraud recovery fraud and makes them less likely to report in the future (and may discourage others from reporting).[63]

How we talk about fraud

It is important to recognise that the terminology used can play a critical part in how society views fraud and this may well influence a victim's decision about whether or not to report it. For instance, whilst the term `scam' is used quite commonly, it can imply something that is a bit of a game and that maybe the victim was partially responsible.

The language of scams

'The word "scam" not only minimises the perceived financial detriment and personal impact a consumer faces but also gives a sense that there is a level of culpability or contributory negligence. This further decreases the already low probability of such a fraud being reported. It is perceived as being "only" a scam and the victim feels embarrassed, ashamed or guilty'.

(Trading Standards Institute[64])

'Words such as "scam", "con", "swindle", "bamboozle" and "cheat" are sometimes used to describe fraud. The slang nature of these terms can often hide the seriousness of the crimes they represent. The effects of fraud can be extremely harmful and are not limited to depriving individuals and businesses of their money, and… the impact on individual victims including the most vulnerable within our society, will be financial and can also include social harms and trauma.'

(National Fraud Authority[65])

Processes for reporting fraud

If a consumer thinks that they are a victim of a fraud, or are concerned that a fraud is taking place, it is essential that they know how to report it and who to contact. The channels for doing so consist of Action Fraud UK, local police, and local trading standards departments via the Citizens Advice consumer service.

Action Fraud

Action Fraud is the UK's national fraud and internet crime reporting centre, based at the City of London Police. Its website advises that Action Fraud should be the first point of contact if someone has been a victim of fraud.[66] This can be done using its online reporting tool or by phone. There is also a service for carers to report scams on behalf of a vulnerable victim (the victim must be under 17, or have a mental health problem or learning difficulty, or a physical disability). However, people are also free to contact their local police direct if they choose to do so.

Action Fraud should be the first point of contact for victims of fraud

Reports made via Action Fraud are passed to the National Fraud Intelligence Bureau (also based at the City of London Police), where the content is analysed to determine if there are other reports concerning the same suspect(s) and if there is an opportunity for the crime to be investigated by a UK Police force. If the report exhibits viable lines of enquiry it is sent to the relevant local police force for possible investigation. This depends on whether the suspect is likely to be traceable and there is an opportunity for enforcement. In addition, reports are passed on if it is considered preferable or appropriate for local police to provide a service to the victim, for example, if the person is very distressed and unable to provide a full account of what happened.[vi]

Reports are passed on if it considered appropriate for local police to provide a service to the victim

People are routinely notified by Action Fraud if a report is passed on to a local police force, and given their contact details. However, not all fraud reports are investigated by local police forces as much depends on their resources and priorities.

Action Fraud changed its processes in May 2014 so that people are also notified in situations where it has decided not to pass on the report to a local police force (normally 28 days later). In these circumstances, people are informed that the report could not be placed with local police at this point in time but that this may change in the future. Action Fraud passes on the reports it receives to the National Fraud Intelligence Bureau, and these are put together with other intelligence, which can lead to subsequent action.

The police in Scotland are not currently part of Action Fraud. However, Action Fraud does not make a distinction between fraud reports it receives as long as there is a UK aspect. If it appears that an offender is based in Scotland, for example, Action Fraud will notify Scottish police.

It is understood that Action Fraud is looking at how its service and communications with the public can be improved to achieve a better understanding of what can and can't be done. This is welcome as it is crucial that everyone who calls Action Fraud is routinely sent a clear and easily understandable response that explains what is happening: either that a report has been sent to a local police force; or that it was not possible to do so at the present time but their information will be kept 'live' and may be followed up in future. Callers should also be signposted to other possible sources of information and advice.

Citizens Advice consumer service and trading standards

The Citizens Advice consumer service provides confidential and impartial advice on consumer issues across the UK, including advice for consumers who have lost money because of a fraud or scam. The service has an agreement with trading standards services to help consumers to report a problem to them. People can contact the consumer service by phone or online by completing a webform. The service's website also advises people to contact Action Fraud if they have been targeted by a scam or know someone who has been targeted.

If someone contacts their local Citizens Advice bureau for advice about a potential fraud, they may be signposted to contact the national consumer service. The service advises anyone who has lost money because of a scam to get in contact as the information can be used by trading standards services to help stop other people becoming victims. The consumer service advisers undergo intensive training to spot key triggers in conversations with clients in order to identify potential criminal activity and how to elicit further information if it is required. The advisers will assess the information provided by callers and work out whether to pass it on to trading standards. (In some situations, more than one local TS may need to be alerted.) Trading standards departments are sent details of all issues reported by consumers and, in some cases, trading standards may be able to help and will contact the consumer directly if this is the case.

The Citizens Advice consumer service provides confidential advice to people who have lost money because of a scam

The information provided by callers may be passed on to other bodies as well as trading standards with the powers to take action against the trader. In some instances, consumer service advisers may also signpost clients to contact Action Fraud and/or other organisations such as Age UK and the Samaritans for further support.

Where it is clear that someone is calling from somewhere in Scotland, the service would normally route them to its Scottish call centre where advisers have an affinity with Scottish consumers. The centre operates in the same way as other parts of the consumer service. When local trading standards departments receive a referral from the Citizens Advice consumer service, they decide what action if any to take depending on local priorities and

resources. Cases where criminality is suspected or where ‘vulnerable consumers’ are involved are likely to be high on their priority lists. Local trading standards can also decide to refer to and work in partnership with the police but this depends on local relationships.

Banks and card companies

If a customer calls their bank or card company to report a fraud on their account and the matter is resolved by the company (for example, where the customer’s account is reimbursed), it can still be reported to Action Fraud. Customers should report all suspected fraud to Action Fraud, according to the BBA. Banks share crime information bilaterally with the National Fraud Intelligence Bureau (NFIB), or pass data to Financial Fraud Action UK (as part of an industry arrangement that takes bulk fraud data from banks and shares regularly on their behalf with the NFIB).

04

The nature and extent of fraud

What types of fraud are being committed?

Fraud covers a very wide spectrum of financial abuse. Below are brief descriptions of just some of the major types of fraud currently being committed against individuals. It is also important to note that consumers may well experience different types of fraudulent activity from the same fraudster. For example, what starts as a romance scam on an online dating site could become an investment fraud if someone is persuaded to send money for bogus shares.[67]

Consumers may well experience different types of fraud from the same fraudster

The list below of examples of fraud against individuals is not intended to be comprehensive as the various types of fraud taking place are too numerous to set out in full. Moreover, both the types of fraud taking place and the methods used can change over time, often rapidly, depending on what opportunities are identified by fraudsters. A more detailed list of types of fraud can be found on the Action Fraud website.[68]

(The sources for the descriptions below include Action Fraud[69], Financial Fraud Action UK[70], the Home Office[71], the Centre for Counter Fraud Studies at the University of Portsmouth[72] and the Trading Standards Institute.[73])

Examples of fraud against individuals

Account takeover: A fraudster poses as a genuine customer, gains control of an account (such as bank, credit card, email and other service providers) and then makes unauthorised transactions. Online banking accounts are usually taken over as a result of methods such as phishing or malware.

Advance fee fraud: Fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise. Types of advance fee fraud include: clairvoyant or psychic scams; dating or romance scams; fraud recovery fraud; inheritance fraud; lottery, prize draw and sweepstake scams; and rental fraud.

Bogus tradesmen or 'doorstep crime': People are called on in person at home and offered repairs or maintenance or goods or services. It may involve pressure selling; unfair contracts; or

overpriced, substandard or non-existent home maintenance or improvements. Fraudsters may claim to have carried out work that has not been done, and make false statements about why the work is required or their membership of trade associations.

Bogus websites: Bogus websites, often purportedly government or regulatory sites, offering services such as passport renewal or driving license applications, usually with an additional fee (or a fee, instead of being free).

Clairvoyant fraud: Apparent psychic or clairvoyant fraudsters approach people by email, post, telephone or face-to-face to tell them something about their future, and ask for money to provide a solution or information.

Council tax: This involves emails that claim to be from local government and state that residents are eligible for a council tax refund. The messages ask for bank and credit card details in order to process the refund but the information is used to take money from the person's account.

419 letter scams: People are contacted by email or letter from someone claiming to be a foreign government official asking them to help transfer money to an overseas bank account in return for a percentage of the amount transferred. But there is no money to transfer and, if the person responds, they will be asked to pay fees allegedly to release the money. The name is derived from Section 419 of the Nigerian Criminal Code.

Fraud recovery fraud: Former fraud victims are told the money they have lost can be recovered by what is allegedly a legitimate organisation. If someone responds, they will be asked for various fees, and they may also be asked for details of their bank account so that the money recovered can be paid into it but instead money will be taken from the account.

Holiday club fraud: Someone is told they have won a 'free' holiday or are pressured into signing a contract for a holiday club. Both can be scams for a bogus holiday club. When the person wants to book a holiday, they may be told that destinations are neither guaranteed, nor available.

Identity theft: Someone's personal details are stolen, and **identity fraud** is when those details are used to commit fraud. It may involve *card ID theft*: when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over someone else's card account. *Third-party application fraud* occurs when criminals use stolen or fake documents to open an account in some else's name.

Inheritance fraud: Someone is told, often via email or letter, by someone claiming to be a legal official that they could receive a large inheritance. The fraudster may say that the lawyer administering the inheritance has been unable to identify the dead person's relatives and that, as the intended victim shares the same family name, they

could be paid the inheritance. The victim will be asked to pay fees upfront and they may also be asked for their bank details, which can then be used by the fraudster.

Investment fraud: Share sales, wine investments, boiler rooms, land banking and carbon credits are commonly used by fraudsters to target potential investors. People may be promised high returns but what is being sold is either worthless or non-existent. Pension liberation fraud is another form. This entails a transfer of a scheme member's pension savings to an arrangement that will allow them to access their funds before the age of 55. This can be illegal where members are misled about key consequences of entering such arrangements.

Mass marketing fraud (MMF): This involves unsolicited or uninvited contacts, usually by e-mail, letter, phone, or through advertisements, with the intention of defrauding people. MMF includes some of the types of fraud listed here, such as investment fraud and '419 letter' scams, as well as many other types of fraud such as fake lotteries and sweepstakes, fake charity donations, and romance and dating fraud.

Plastic card fraud: This involves the compromise of any personal information from credit, debit or store cards. The information stolen from a card, or the theft of a card itself, can be used to commit fraud such as to buy goods or services or to obtain unauthorised funds. Plastic card fraud can also include 'card not present' fraud, such as the use of a card online, over the phone or by mail order, and counterfeit card fraud.

Private **pension liberation** is a relatively recent fraud

Methods used

It can be difficult to separate out types of fraud from the methods used, and the list above includes some of the methods used to contact potential victims and to commit fraud, such as the use of emails, letters (including mass mailings), and calling on people at their homes**.**

The growth in use of the internet means that fraudsters frequently employ online methods to target people and these include:

Phishing: A method used to access valuable personal details, such as usernames and passwords. It involves the use of bogus communications – emails, instant messages or text messages – that may appear to be authentic communications from legitimate organisations. Links within the message may direct people to a hoax website where their personal details may be requested, which can then be used to commit fraud.

Spam emails: Messages are sent to multiple email addresses to try to gain personal information that can be used to commit fraud, such as credit card and identity fraud**.**

Malware: This is malicious software that consists of programming, for example code or scripts, designed to disrupt the performance of PCs, laptops, handheld devices, etc. Malware can also collect information or data from infected devices and pass them on to another device. It can involve `scareware' that imitates valid software to convince users that an upgrade is needed, which will entail a fee but will be non-existent. Or it could involve ransomware which copies personal files or photos, and a demand is then issued for money for their return for the images or files.[74]

For example, the Information Commissioner's Office (ICO) has drawn attention to emerging evidence that the threat posed by unsolicited texts to smart phones is growing, as these texts can lead to malware being installed.[75]

Over 5% of **plastic card owners** were victims of card fraud in 2012/13

What is the extent of fraud?

Limitations of official statistics

It is not possible to give a comprehensive and reliable estimate of the extent of fraud carried out against older people and other consumers in the UK because of the limitations of official statistics.

The former National Fraud Authority (NFA) used to publish an Annual Fraud Indicator, which set out estimates based on a compendium of fraud loss indicators drawn together to illustrate the possible scale, prevalence and cost of fraud. It also highlighted gaps in identified and hidden or undetected fraud. This information is no longer available in the form developed by the NFA.

Statistics on certain types of reported fraud offences in England and Wales are published regularly by the Office for National Statistics (ONS) – see below.

Fraud is not included in the main Crime Survey for England and Wales (CSEW) estimates produced by the ONS. However, the CSEW includes supplementary modules of questions on victimisation across a range of fraud and cyber-crime offences, including plastic card and bank/building society fraud. These are currently reported separately from the headline crime estimates.[76]

The 2013/14 CSEW showed that 5.1 per cent of plastic card owners were victims of card fraud in the previous year, with a statistically significant rise from the 4.6 per cent estimated in the 2012/13 CSEW. The current increased level of

victimisation remains higher than more established offences such as theft from the person and 'other' theft of personal property.[77]

Separate analysis by the ONS (based on the 2012/13 CSEW) showed that together, plastic card fraud and bank and building society fraud could have contributed between 3.6 and 3.8 million incidents of crime to the total number of CSEW crimes in this survey year. These numbers provide an approximate indication of the scale of these offences that are not covered in the headline estimates each year. However, according to the ONS, these are based on some simple assumptions given the current absence of data on the number of times respondents fell victim within the crime reference period.[78]

The ONS aims to expand the Crime Survey for England & Wales to include fraud and cybercrime

The ONS is currently exploring the feasibility of extending the main victimisation module in the CSEW to cover elements of fraud and cybercrime. According to the ONS, this work will be extensive with the aim of questions being implemented in the 2015/16 questionnaire.[79]

ONS statistics are based on fraud reports from Action Fraud. Hosted by the City of London police, Action Fraud has been responsible for central recording of fraud offences across the UK since April 2013, which were previously recorded by

Statistical conceptual issues

The ONS has drawn attention to a range of conceptual challenges that need to be addressed:

Counting incidents: Plastic card or bank account fraud often involve separate 'events' (for example, card purchases at different retailers on different days) and a clear set of rules for counting incidents would need to be established.

Identifying and counting victims: For example, in bank and credit card (cyber-enabled) fraud, it may be unclear whether the victim is the bank or financial institution who suffers the loss or the customer.

Identifying where the crime took place: While it is often possible to identify where the victim(s) reside, it is often not possible to identify where the offence originated. Only those which take place within England and Wales should be counted according to the ONS.

The means for criminals to attempt to commit this type of crime on a grand scale: A single act of uploading a computer virus or sending a malicious e-mail may impact on thousands of people and could (in theory) result in thousands of crimes being recorded.[80]

individual police forces. Due to this change, the ONS warns against making like for like comparisons between fraud offences recorded during 2013/14 with previous years. Action Fraud collects statistics on crime across the UK; the information currently available on its website is available by county and region and over the last few months.

It should also be noted that the ONS fraud statistics for England and Wales do not include trading standards prosecutions. However, the Trading Standards National Scams Team is currently working on this issue at a national level.

Moreover, the recent national audit of the integrity of police-recorded crime data carried out by HM Inspectorate of Constabulary did not examine fraud offences – the report referred to Action Fraud having taken responsibility for recording fraud reported by victims in police force areas.[81]

With regard to Scotland, fraud is not currently included in the Scottish Crime and Justice Survey (SCJS).[82] The SCJS does not ask specific questions on general fraud in the victim form as there are a number of issues with measuring this particular type of crime and therefore fraud is not included in any of the SCJS crime statistics. There is some limited information in the SCJS 2012/13, which estimated that four per cent of adults had experienced card fraud in the 12 months prior to interview. Around one per cent of adults had been a victim of identity theft. However, Scottish Government statistics on police recorded crime include fraud.[83]

While currently this is the only information on fraud in the SCJS, we understand that the Scottish Government is closely monitoring the evolving work being undertaken in ONS to consider further development of questions on fraud and cyber crime for the CSEW.[vii]

Reported fraud offences in England and Wales

We have drawn together some key relevant statistics that provide indicators about the extent of certain types of reported fraud against individuals.

A total of 211,344 fraud offences were recorded in England and Wales in the year ending March 2014, according to ONS figures.[84] However, this figure includes fraud against organisations, such as the DWP and HMRC, as well as reported offences committed against individuals. We have therefore tried as far as possible to set out on page 34 the data on fraud offences that appear most likely to have been committed primarily or largely against individuals (according to descriptions of offences published by the Home Office[85]). However, some may include offences committed against organisations as well as individuals, such as offences involving computer malware.

An estimated **165,488 fraud offences** against individuals were recorded in England and Wales in 2013/14

Recorded fraud offences in England and Wales, 2013/14:[86]

Non-investment fraud	
of which:	
Online shopping and auctions	*41,645*
Consumer phone fraud	1,213
Door to door bogus tradesmen	*5,673*
Other consumer non investment fraud	15,288
Computer software service fraud	*10,782*
Ticket fraud	4,250
Advance fee payments	
of which:	
'419' Advance fee fraud	949
Lottery scams	*1,580*
Dating scam	2,037
Fraud recovery	*1,329*
Inheritance fraud	711
Rental fraud	*2,510*
Other advance fee frauds	20,495
Lender loan fraud	*7,691*
Banking and credit industry fraud	
of which:	
Cheque, plastic card & online bank accounts	17,426
Application fraud (excluding mortgages)	*3,007*
Mandate fraud	2,284
Computer misuse crime	
of which:	
Computer virus/malware/spyware	10,731
Hacking - personal	*2,462*
Hacking - social media and email	5,896
Hacking - PBX/dial through	*435*
Hacking extortion	1,414
Financial investments	
of which:	
Share sales or boiler room fraud	1,619
Pyramid or Ponzi schemes	*343*
Prime bank guarantees	22
Time shares and holiday club fraud	*343*
Other financial investment	2,053
Pension fraud	
of which:	
Pension fraud committed on pensioners	44
Pension liberation fraud	*701*
Charity fraud	555
TOTAL	**165,488**

Other fraud statistics

Doorstep crime

In 2011 a National Audit Office (NAO) report identified doorstep crime as a major source of detriment but the report also pointed out that there are no reliable figures available to estimate the impact of this on consumers.[87]

In October 2013, North Yorkshire Trading Standards was tasked by the National Tasking Group of the National Trading Standards Board to undertake a project examining current efforts to tackle doorstep crime in England and Wales through enforcement, intelligence and prevention. According to the report on this project, there are currently around 17,000 doorstep crime reports to trading standards annually in England and Wales. But this represents only 10-20 per cent of incidents that are actually occurring, and the true number taking place annually was estimated at between 85,000–170,000.[88]

There are an estimated 85,000–170,000 doorstep crimes annually in England & Wales

The project report made a series of recommendations including the need for improvements in data recording; a number of initiatives to prevent doorstep crime and raise public awareness; and academic research including typologies of offenders and victims (we understand that a range of activities are being carried out as a result).

Mass marketing fraud

Mass marketing fraud is becoming a more serious, complex and growing crime in the UK and internationally, according to the ONS.[89]

In a focus project on property crime which included mass marketing fraud, the 2011/12 CSEW asked respondents in England and Wales if they had personally received any emails, texts, letters or phone calls from an individual or a company they have never heard of before that might have involved a request for money (referred to as unsolicited communication). The results showed that:[90]

- A full 56 per cent of adults had received an unsolicited communication in the previous 12 months; only a very small percentage actually fell victim.
- Those receiving unsolicited communications were more likely to be aged 25 to 44; highest rates of receipt were found among those aged 25-34 (63 per cent) and 35-44 (61 per cent). Those aged 75 and over were less likely to receive such communications (40 per cent).
- Of those who had used the internet in the last 12 months, 62 per cent had received an unsolicited communication compared with 37 per cent of adults who had not used the internet in the last 12 months.

56 per cent of adults received an unsolicited communication in the previous 12 months

Less than one per cent of adults who received either a communication involving a lottery, guaranteed high investment return or romance fraud, sent or transferred money. But, as the ONS noted, these may represent underestimates of the true prevalence of victimisation as some victims may have been too embarrassed to disclose this information.[91] Other limitations to these findings have been pointed out elsewhere, for example, it appears that the scenarios presented to interviewees did not reflect the full diversity of this type of fraud. In addition, the survey did not account for people who became victims through searching on the internet for products and services, as opposed to those targeted by unsolicited communications.[92]

Less than one per cent of those who received a communitcation sent or transferred money. But this may be an underestimate due to under-reporting

It is worth noting that mass marketed scams had been one of the OFT's five priority areas with a focus on coordination, enforcement action and consumer education. The OFT also commissioned quantitative and qualitative consumer research on scams as part of its work.[93]

Cyber crime

A review of cyber crime for the Home Office in 2013[94] identified a number of challenges to improving understanding of cyber crime including the following:

- Lack of recording mechanisms that accurately distinguish between online and offline crime.
- Under-reporting of cyber crime from the public and businesses and a lack of awareness that some cyber incidents are actually crimes (although not all are).
- Inconsistencies in the measurement and definition of cyber crime within the relevant research.
- Information from industry sources often lacks transparency and comparability.
- Few methodologically sound surveys of victims exist.
- Cyber crime can be undertaken on a large scale, potentially resulting in a relationship between victims and offenders that is very different to 'offline' crime.
- Cyber crime is global in nature; it is not constrained by national boundaries.

Cyber crime is global in nature – it is not constrained by national boundaries

The review identified a number of limitations regarding the existing evidence base on cyber crime. For example:

- It did not distinguish between online and offline crimes.
- Some surveys were based on small, non-random and unrepresentative samples, meaning that findings could not be inferred to the wider population.
- Ambiguities and inconsistencies in measurement, definitions and methodology.
- Lack of transparency in methodologies (particularly amongst industry reports).
- In some cases, a complete lack of UK-based evidence.

Identity fraud

The misuse and abuse of personal data was described by Cifas as the most severe challenge to organisations and individuals. Their figures show that identity related crimes accounted for over 60 per cent of confirmed fraud reported to Cifas in 2013, repeating the patterns of previous years.[95]

Reports received by Citizens Advice Scotland Consumer Helpline about bogus selling rose by 14 per cent in 2013/14 compared with the previous year.[96] Unsolicited contact, either by telephone, email, post or doorstep, is by far the most common method (60 per cent) used by bogus sellers. Services such as investments and financial advisers represented 15 per cent of all bogus selling reports. Other areas with a high proportion of calls were lotteries (11 per cent), insurance (9 per cent), home maintenance (per cent) and computing (6.5 per cent).

Improving the evidence base

It is abundantly clear that urgent improvements are needed in the recording and publication of statistics on the prevalence of fraud against individuals in the UK.

As stated in a research article this year:

'There also need to be more regular and nuanced surveys of the prevalence of victimisation for fraud among the general public.

This could provide better information on trends in different types of fraud, the modus operandi of fraudsters, the characteristics and needs of victims.

Such surveys of appropriate depth would also provide data on any changes in why victims might be falling for such scams. This wide range of data would not only aid investigatory activities but also the prevention work of anti-fraud bodies.

The technological revolution will increase the risk of more people becoming victims

More in-depth research should also be conducted on some of the more common scams, for it is clear the underpinning technological revolution, which has occurred in recent years is likely to further increase the risk of more people becoming victims as access to and ease of use of the internet continues to rise all over the world.' [97]

05

Legal aspects

This section discusses legal regulation of fraud. The criminal law in England and Wales is found in two places: the Fraud Act 2006 and the Consumer Protection from Unfair Trading Regulations 2008 which implemented the Unfair Commercial Practices Directive. There is no offence of using either postal or electronic communication for fraudulent purposes, although there are offences of sending indecent material via these channels, which seem to be prosecuted regularly.

The Fraud Act 2006 and Consumer Protection from Unfair Trading Regulations 2008 are key

Enforcement of the criminal law is split between police forces, Action Fraud and the Crown Prosecution Service who are responsible for the general criminal law, and trading standards services and the Competition and Markets Authority (CMA) who have responsibility for enforcing the Unfair Trading Regulations. As will become clear, the criminal offence under the Unfair Trading Regulations has a wider scope than that under the Fraud Act.

The Fraud Act 2006

Unlike Scotland (see below) the law of England and Wales did not have a common law offence of fraud, only conspiracy to defraud. A number of statutory deception offences were created by the Theft Acts but, when the Law Commission looked at the area in 2002, they took the view that the problem with the current offences involving fraud was that, while conspiracy to defraud was too wide in its scope, in that it included agreements to do things which were rightly not criminal per se, the statutory offences were too narrow and particularised and failed to capture some conduct which should be criminal.

The Law Commission's proposals led to the Fraud Act 2006, which aimed to reform the law of fraud in England and Wales by simplifying it and making it a more effective tool for prosecutions. It did this by introducing a new general offence of fraud which can be committed in three different ways:

1. By a false representation
2. By failing to disclose information which a person is under a legal duty to disclose
3. By abuse of a position

For our purposes, fraud by false representation is the most important provision. In order to establish this offence, a person must dishonestly make a false representation, and intend, by making such a representation to either make a gain for themselves or another or to cause loss to another or expose them to the risk of loss.[viii] A representation is false if it is untrue or misleading and the person making the representation knows that it is untrue or misleading.[ix] *UAE v Allen*[x] held that a representation had to be capable of being expressed as a statement of the past or present; a statement as to the future might take effect as a contractual promise, but it could not come within the legal classification of a representation.

Fraud by false representation is the most important provision

There are no obvious legal problems with prosecuting fraud. It would not, for example, be possible for a person accused of fraud to argue that the victim consented because of the deception engaged upon by the fraudster. There is, however, a question over the relative priority given to fraud investigations by police forces.

The fraud offence in Scotland

There is a common law offence of fraud in Scotland which is relatively simple and has a wide coverage. The offence is the bringing about of any practical result by a false pretence where the accused is aware of the falsity of the pretence and has the intention of bringing about the practical result. The victim must have been deceived by the false pretence and acted on the basis of it. The false pretence can be express or implied and omissions are also covered. Almost any practical result will be sufficient to constitute fraud, although the victim's conduct must have been caused by the false pretence.

The Unfair Trading Regulations 2008

These Regulations make it a criminal offence for a trader to engage in misleading actions or omissions.[xi] A practice is misleading under Regulation 5 if it contains false information and is therefore untruthful in relation to any of the matters specified in the Regulations: or if it or its overall presentation in any way deceives or is likely to deceive the average consumer in relation to any of the matters specified in the Regulation, even if the information is factually correct; and it causes or is likely to cause the average consumer to take a transactional decision s/he would not have taken otherwise. The matters referred to in the Regulations include the existence or nature of the product, its main characteristics and the extent of the trader's commitments.

The Regulations make it a criminal offence for a trader to engage in misleading actions or omissions

A misleading omission is a commercial practice which omits or hides material information or provides it in a manner which is unclear, unintelligible, ambiguous or untimely or conceals the fact that it is a commercial practice. The result must be to cause or to be likely to cause the average consumer to enter

into a transactional decision which they would not otherwise have done. Material information includes the material that an average consumer would need before entering into such a transaction and any material that is required to be provided under EU law.

Regulation 6 goes on to set out explicitly further information which is considered material, such as the identity and address of the trader and the terms and conditions of delivery.

In addition, Schedule 1 sets out a list of 31 practices which are in all circumstances considered unfair. These include persistent unwanted solicitation by telephone or e-mail (although not post) and pretending that a prize has been, or can be, won, when either it is not available or taking any action to claim the prize will involve the consumer paying money or incurring a cost.[xii]

Unfair practices include persistent unwanted solicitation by phone or email and pretending that a prize has been won

A 'transactional decision' means any decision taken by a consumer, whether it is to act or to refrain from acting, concerning:

- whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product; or
- whether, how and on what terms to exercise a contractual right in relation to a product.

The offences contained in the Unfair Trading Regulations are wider than the offences under the Fraud Act 2006. First, under the Fraud Act, there has to be intention to deceive. This is not required under the Regulations. Secondly, the representation under the Fraud Act must be untrue or misleading. The Regulations make it clear that even factually correct information may be presented in such a way as to be misleading. Thirdly, the case law cited above suggests that representations can only refer to the past or present, not the future. The Regulations do not seem to be so restricted.

The offences in the Unfair Trading Regulations are wider than those in the Fraud Act

As mentioned above, the provisions in the Regulations are enforced by trading standards and the CMA, although trading standards has a duty to enforce this law while the CMA has only a power. The CMA sees criminal prosecutions as a secondary part of its enforcement armoury but it stresses that it will use them and act decisively where appropriate.[98] The prosecution record over the last five years for Regulations 5 and 9 (which are the main subject of this research[xiii]) is noticeable in that there are only about 130 prosecutions annually and that the two most common subjects are house maintenance and related issues, and motor transport (primarily selling second hand cars). In other words, these provisions do not appear to have been used regularly against mass marketing fraud.

The most common **unfair trading** issues are **house maintenance** and **motor transport**

The 'average consumer' and 'vulnerable consumer'

An important concept within the Regulations is the meaning of 'average consumer'. In general, an average consumer is expected to be reasonably well informed, reasonably observant and circumspect.[xiv]

However, the Regulations also refer to 'vulnerable consumers':

> *'Regulation 2(5) states that, when determining the effect of a practice on an average consumer where a clearly identifiable group of consumers is particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, and where the practice is likely to materially distort the economic behaviour only of that group, a reference to the average consumer shall be read as referring to the average member of that group.'*

Right to redress

There have been recent amendments to the Consumer Protection from Unfair Trading Regulations with the insertion of a new part 4A which replace enforcement under the Misrepresentation Act 1967. This provides consumers with a right to redress if, among other things, a trader engages in a misleading practice.[xv] The consumer has a right to damages for loss, alarm, distress, physical inconvenience or discomfort which would not have occurred if the prohibited practice in question, in this case the provision of misleading information, had not occurred (Regulation 27J).

Some consumers are particularly vulnerable because of their mental or physical infirmity, age or credulity

Other relevant legislation

There are other aspects of the legal framework that are relevant in the context of fraud, some of which are outlined below. In addition, the Postal Services Act 2000 and the Regulation of Investigatory Powers Act 2000 are relevant in the context of mail fraud, together with the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Communications Act 2003 and the Data Protection Act 1998.

Enterprise Act 2002

The CMA also has powers under Part 8 of the Enterprise Act 2002 which allows it to apply to the courts for an enforcement order to stop a business from breaching, among other provisions, the Unfair Trading Regulations where that breach harms the collective interests of consumers, either generally or as a specified group. The CMA says that enforcement action may be appropriate where it has determined that breaches of law point to systemic failures in a market, where changing the behaviour of one business would set a precedent or have other market-wide implications, where there is an opportunity to set an important legal precedent or where there is a strong need for deterrence or to secure compensation for consumers.[99]

Computer Misuse Act 1990

Certain types of mass market fraud may be covered by the Computer Misuse Act 1990. Section 1 makes it an offence for a person to cause a computer to perform any function with the intent to secure any program or data held in such a computer. This provision does not seem to be used very often. A Home Office study concluded that:

> *'Between 2007 and 2012 initial proceedings were taken against 101 people and 88 people were sentenced with a primary offence under the Act. The seemingly low level of sentencing under the [Computer Misuse Act] reflects the fact that individuals are being proceeded against for cyber offences under other Acts such as the Fraud Act …'* [100]

From the point of view of the Information Commissioner:

> *'Computer scams may involve someone trying to gain access to your computer remotely to control it or steal sensitive information. These calls are not direct marketing, and we refer information to law enforcement agencies where we uncover instances of potential fraud or computer misuse.'* [101]

Safeguarding

There is an established safeguarding concept or principle which implies that some people who are particularly at risk in a variety of ways should have statutory protection arrangements in place.

England and Wales

The Care Act 2014 covers England and Wales and took effect in April 2015. It sets out how local authorities and other health and care services should protect adults at risk of abuse or neglect. Safeguarding becomes a specific statutory duty, and local authorities are required to set up a Safeguarding Adults Board in their area.[102]

The Act requires local authorities to make enquiries, or ask others to make enquiries, when they think an adult with care and support needs may be at risk of abuse or neglect in their area and to find out what, if any, action may be needed (s.42). This applies whether or not the authority is actually providing any care and support services to that person.

Abuse includes financial abuse, and this includes:

a) *'having money or other property stolen,*
b) *being defrauded,*
c) *being put under pressure in relation to money or other property, and*
d) *having money or other property misused.'*

Scotland

Under the Adult Support and Protection (Scotland) Act 2007, local councils must make inquiries about a person's well-being, property or financial affairs if it knows or believes that the person is an adult at risk, and that it might need to intervene in order to protect the person's well-being, property or financial affairs. It requires councils and a range of public bodies to work together to support and protect adults who are unable to safeguard themselves, their property and their rights, balancing the need to intervene with an adult's right to live as independently as possible.[103]

Safeguarding is the **principle** that people who are particular**ly at risk** should have **statutory protection** in place

06

Conclusions

Different types and tactics

Fraud can take many forms and the term covers a wide spectrum of financial abuse. A wide range of methods, tactics and communications channels are used to target people but the advent of the internet has clearly provided fraudsters with far greater opportunities to target many more people than was previously the case. It is especially worrying that some people, particularly consumers in vulnerable circumstances, may be repeatedly targeted and are often put on 'suckers lists' for use by fraudsters in the UK and internationally.

It is especially worrying that some people in vulnerable circumstances are repeatedly targeted

The available evidence base shows that the tactics used by fraudsters include befriending and 'grooming', for example through personal contact on the doorstep and online communications. However, threats and intimidation are also among the tactics used to commit fraud.

Older people at risk

The lack of a sound and up-to-date evidence base makes it difficult to assess the extent to which older people are being targeted by fraudsters and then become fraud victims. However, it is clear that older people are likely to be at risk of being targeted for certain types of fraud. Moreover, some older people are likely to be particularly at risk as a result of circumstances such as social isolation or cognitive impairment, and/or exposed to fraud such as doorstep crime.

At the same time, it is vital to understand that anyone can be targeted by fraudsters and become a victim, including people who consider themselves to be financially sophisticated. It can also be very difficult for people to determine if fraud is being carried out; for example, if messages are from legitimate organisations or whether websites are authentic or fake. Also, some people may be especially vulnerable to fraud due to financial or other pressures that cause them to make decisions under stress.

Prevalence and evidence

The evidence base on the prevalence of fraud against consumers in general is confusing, patchy and ultimately unsatisfactory, including in relation to older people. For example, although use of the internet is lower among older people than others in the population, this is changing. However, much of the evidence base about who is being targeted for online fraud predates the recent rapid growth in internet use. Moreover, it is extremely difficult to track changes in the types and extent of fraud over time.

Consequently, there are serious and urgent questions that need to be addressed about the inadequacy of UK official statistics on fraud with regard to individuals, particularly in relation to the Crime and Justice Survey for England and Wales and the Scottish Crime and Justice Survey.

Victims' experiences

Similarly, evidence about the circumstances of fraud victims is worryingly patchy. For many older people the effects of being a fraud victim can be highly damaging. People on a fixed income may not be able to replace the financial loss, and some could lose their entire savings. The implications for people's physical and mental health often vary between individuals but the impact should not be under-estimated.

The effects of being a victim of fraud can be serious and long-lasting for the individual and their families. Far greater attention needs to be paid to the experiences of older people and others who have been targeted by fraudsters and may then have become victims.

The effects on older fraud victims can be highly damaging

Under-reporting

Under-reporting of fraud is a major problem and self-blame and embarrassment on the part of victims are significant factors but not necessarily the only reasons. More needs to be known about why some people report fraud and others do not, about the factors that may cause people to be particularly at risk of becoming victims, and about the effectiveness of prevention measures and reporting processes.

Priorities and resources

The research has not identified significant gaps or omissions in the legal framework. But there are questions that need to be addressed about the priority given to investigating and tackling fraud against individual consumers by the relevant bodies involved, and the resources that are allocated to these activities.

Notes

i These figures are from the scams survey by Populus for Age UK, which took place between 13 and 15 March 2015. It questioned 1,002 adults aged 18+ in England, Scotland and Wales over the phone.

ii The quantitative research for the FCA involved an analysis by Experian of the geographic, demographic and socio-economic profile of investment fraud victims using 11,359 individual records.

iii This research involved initial interviews with more than 11,200 people and 1,900 detailed follow-up interviews with people who reported that they had been a victim of a scam, or knew someone who had been a victim, or had been a target of a scam.

iv Where would-be tenants are deceived into paying an upfront fee to rent a property that turns out not to exist, or is already rented out, or is rented to multiple victims at the same time.

v A door-to-door fraud where criminals offer discounted energy credits to households who pay for their electricity in advance through a key or card that they put into their meters. The customer may then pay twice: once to the criminal and again to their energy supplier. *Annual Fraud Indicator*, National Fraud Authority (2013).

vi Telephone interview with National Fraud Intelligence Bureau, 13 November 2014.

vii Email 6 November 2014

viii Fraud Act 2006 s. 2(1)

ix Ibid, s. 2(2)

x [2012] EWHC 1712 (Admin).

xi Consumer Protection from Unfair Trading Regulations 2008/127 Regulations 5-6

xii Ibid., Schedule 1, paras 19, 26 and 31

xiii There have been some prosecutions for breach of Regulations 6 and 10 and for breaches of Schedule 1. There were 42 for 2013-14 in relation to Regulations 6 and 10 and 58 for Schedule 1. The recording categories do not explicitly cover mass market fraud.

xiv Ibid., Reg 2(2)

xv Consumer Protection from Unfair Trading Regulations 2008/127 Regulation 27A

References

1 *The psychology of scams*, University of Exeter and the OFT, 2009

2 *Scammed and dangerous: the impact of fraudsters*, Citizens Advice Scotland, 2014

3 *A better deal for fraud victims: Research into victims' needs and experiences*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth and National Fraud Authority, 2009

4 *Fraud typologies and victims of fraud: Literature review*, Button M, Lewis C and Tapley J, National Fraud Authority and the Centre for Counter Fraud Studies, 2009

5 *A better deal for fraud victims: Research into victims' needs and experiences*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth and National Fraud Authority, 2009

6 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

7 Ibid.

8 *Later Life in the United Kingdom*, Age UK, October 2014

9 *The psychology of scams*, University of Exeter and OFT, 2009

10 *Fraud typologies and victims of fraud: Literature review*, Button M, Lewis C and Tapley J, National Fraud Authority and the Centre for Counter Fraud Studies, 2009

11 *Scammed and dangerous: The impact of fraudsters*, Citizens Advice Scotland, 2014

12 *Fraud typologies and victims of fraud: Literature review*, Button M, Lewis C and Tapley J, National Fraud Authority and the Centre for Counter Fraud Studies, 2009

13 www.southlanarkshire.gov.uk/press/article/993/fraudster_targeted_south_lanarkshire_suckers

14 *Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance*, Fischer P, Lea S E G, Evans K M, Journal of Applied Social Psychology, 43, 2013

15 Ibid.

16 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

17 North Yorkshire County Council press release, 14 January 2013

18 *Scammed and Dangerous: The impact of fraudsters* (2014), Citizens Advice Scotland

19 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

20 http://www.tradingstandards.gov.uk/events/events-ncw.cfm

21 http://www.actionfraud.police.uk/types-of-fraud/mass-marketing-fraud

22 A *trading standards perspective on unsolicited or nuisance telephone calls*, briefing by Smith B, Trading Standards Institute, (undated)

23 *Online frauds: Learning from victims why they fall for these scams*, Button M et al, Australian & New Zealand Journal of Criminology, Sage, published online 28 March 2014

24 Ibid.

25 *Policy brief: Scams & Think Jessica campaign*, Trading Standards Institute, 2009

26 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

27 http://www.thinkjessica.com/faqs.htm

28 *A better deal for fraud victims: Research into victims' needs and experiences*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth and National Fraud Authority, 2009

29 Ibid.

30 http://www.fca.org.uk/consumers/scams/common-scams/banking-and-online-accounts

31 *Fraud: The facts*, Financial Fraud Action UK, 2014

32 *Scam alert,* Financial Fraud Action UK, 29 October 2014

33 *Fraudscape: depicting the UK's fraud landscape*, Cifas, 2014

34 *Understanding victims of financial crime: A qualitative study with people affected by investment fraud*, NatCen and FCA, 2014

35 Ibid.

36 *A quantitative analysis of victims of investment crime*, FCA, 2014

37 Ibid.

38 *Serious and organised crime strategy*, Home Office, 2013

39 http://www.thepensionsregulator.gov.uk/regulate-and-enforce/pension-scams.aspx

40 *Guardian,* 6 September 2014

41 Ibid.

42 https://www.gov.uk/government/news/pensions-guidance-providers-unveiled

43 *Annual fraud indicator*, National Fraud Authority, 2013

44 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

45 *A better deal for fraud victims: Research into victims' needs and experiences*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth and National Fraud Authority, 2009

46 *Fraudscape – depicting the UK's fraud landscape*, Cifas, 2014

47 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

48 Ibid.

49 *Not a victimless crime: The impact of fraud on individual victims and their families*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth, Security Journal, 27, Macmillan, 2014. Published online 23 April 2012

50 http://www.gmp.police.uk/content/section.html?readform&s=803408449178D82780257961003E0749

51 *Not a victimless crime: The impact of fraud on individual victims and their families*, Button M, Lewis C and Tapley J, Centre for Counter Fraud Studies, University of Portsmouth, Security Journal, 27, Macmillan, 2014. Published online 23 April 2012

52 *Assessment: Financial crime against vulnerable adults*, Social Care Institute for Excellence, 2011

53 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

54 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

55 *Annual fraud indicator*, National Fraud Authority, 2013

56 *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, OFT, 2006

57 Ibid.

58 *Scammed and dangerous: the impact of fraudsters*, Citizens Advice Scotland, 2014

59 *Understanding victims of financial crime: A qualitative study with people affected by investment fraud*, NatCen and FCA, 2014

60 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

61 Ibid.

62 *Understanding victims of financial crime: A qualitative study with people affected by investment fraud*, NatCen and FCA, 2014

63 Ibid.

64 A *trading standards perspective on unsolicited or nuisance telephone calls*, briefing by Smith B, Trading Standards Institute, (undated)

65 *Annual fraud indicator*, National Fraud Authority, 2013

66 http://www.Action Fraud.police.uk/report_fraud

67 *Online frauds: Learning from victims why they fall for these scams*, Button M et al, Australian & New Zealand Journal of Criminology, Sage, published online 28 March 2014

68 http://www.actionfraud.police.uk/a-z_of_fraud

69 http://www.actionfraud.police.uk/types_of_fraud

70 *Fraud: The facts*, Financial Fraud Action UK, 2014

71 *Home Office Accounting Rules for Recorded Crime,* Home Office, April 2014

72 *Fraud typologies and victims of fraud: Literature review*, Button M, Lewis C and Tapley J, National Fraud Authority and the Centre for Counter Fraud Studies, 2009

73 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

74 http://www.actionfraud.police.uk/a-z_of_fraud

75 *Evidence submitted by the Information Commissioner to the House of Commons Select Committee for Culture, Media and Sport*, House of Commons, 636-I, 2013/14

76 *Chapter 1: Property crime: Overview*, Office of National Statistics, November 2014

77 Ibid.

78 Ibid.

79 Ibid.

80 Ibid.

81 *Crime-recording – Making the victim count: The final report of an inspection of crime data integrity in police forces in England and Wales*, HMIC, 2014

82 *Scottish crime and justice survey 2012/13: Main findings*, Scottish Government, 2014

83 http://www.scotland.gov.uk/Publications/2013/06/9697/6#table1

84 *Crime in England and Wales, year ending March 2014, statistical bulletin*, Office for National Statistics, 17 July 2014

85 *Home Office accounting rules for recorded crime,* Home Office, April 2014

86 *Crime in England and Wales, year ending March 2014, statistical bulletin*, Office for National Statistics, 17 July 2014

87 *Protecting consumers: The system for enforcing consumer law*, Report by the Comptroller and Auditor General, House of Commons, 1087, Session 2010–2012, 2011

88 National Trading Standards National Tasking Group Doorstep Crime Report, March 2014

89 http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/focus-on-property-crime--2011-12/rpt---chapter-4.html#tab-Introduction

90 http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/focus-on-property-crime--2011-12/rpt---chapter-4.html

91 Ibid.

92 *Online frauds: Learning from victims why they fall for these scams*, Button M et al, Australian & New Zealand Journal of Criminology, Sage, published online 28 March 2014

93 *Fraud review final report: A consultation response by the Office of Fair Trading*, OFT, 2006

94 *Cyber crime: A review of the evidence*, Home Office research report 75, McGuire, M and Dowling, S, 2013

95 *Fraudscape: depicting the UK's fraud landscape*, Cifas, 2014

96 *Scammed and dangerous: the impact of fraudsters*, Citizens Advice Scotland, 2014

97 *Online frauds: Learning from victims why they fall for these scams*, Button M et al, Australian & New Zealand Journal of Criminology, Sage, published online 28 March 2014

98 *Consumer protection: Guidance on the CMA's approach to use of its consumer powers*, CMA, 2014, available at: https://www.gov.uk/government/publications/consumer-protection-guidance-on-the-cmas-approach-to-use-of-its-consumer-powers

99 Ibid.

100 *Cyber crime: A review of the evidence*, Home Office research report 75, McGuire, M and Dowling, S, 2013

101 http://ico.org.uk/enforcement/action/calls

102 https://www.gov.uk/government/publications/care-act-2014-part-1-factsheets

103 http://www.scotland.gov.uk/Topics/Health/Support-Social-Care/Adult-Support-Protection/National-Priorities

Age UK
Tavis House
1-6 Tavistock Square
London
WC1H 9NA
0800 169 80 80
www.ageuk.org.uk