HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number CBP-07691, 6 September 2016

Scamming and its effect on vulnerable individuals

Lorraine Conway, Djuna Thurley & Tim Edmonds

Contents:

Contents

Contributing authors Sally Lipscombe (overview); Tim Edmonds (financial and investment fraud); Djuna Thurley (pensions); Lorraine Conway (consumer scams)

Summary

This briefing paper is for the backbench business debate on 8 September 2016 on the following motion:

> **SCAMMING AND ITS EFFECT ON VULNERABLE INDIVIDUALS**
>
> Julian Knight
>
> Patricia Gibson
>
> That this House believes that the elderly and vulnerable are a high-risk group from having harm done to their financial, emotional and psychological wellbeing from criminals who target them with scam calls, post and visits; praises the work that trading standards does to combat scams; calls on financial institutions and the communications industry to put in place mechanisms to protect potential victims from scams; further calls on the Government to recognise the threat from scams to victims' ability to live independently; draws attention to the measures proposed by Bournemouth University, the Chartered Trading Standards Institute and National Trading Standards Scams Team on financial harm as useful first steps in tackling such scams; and calls on the Government to make suggestions on further steps to tackle such criminality.

The aim of this briefing paper is to set out why people can be vulnerable to scams, what they can do to protect themselves and what action is being taken by the government and the regulators.

The annual cost of fraud against individuals – including mass marketing fraud and identity fraud – has been estimated at some £9.7 billion. Research conducted in April 2015 by Age UK suggested that 53 per cent of people aged 65+ believed they have been targeted by fraudsters.

Financial investment and fraud

Scams come in many forms, and through different channels, but scams involving false investment opportunities are one of the commonest and some of the most devastating when they involve the life savings of elderly individuals.

The main regulator is the Financial Conduct Authority which has, a statutory objective of "Securing an appropriate degree of protection for consumers".

It seeks to do this in many ways; through consumer information/education programmes such as the ScamSmart scheme and the active investigation and prosecution of suspect activity.

In 2015, the FCA received over 8,500 reports about potential unauthorised activity and sent eight people to jail for a total of 32 years, froze over £2.7 million of assets and returned nearly £1.9 million to victims.

Pensions

Changes in the law in April 2015 gave people aged 55 and over more flexibility over when and how to draw their defined contribution pension savings. The Government said it recognised that people would need help navigating the expanded range of options and therefore introduced a guidance service – Pension Wise. Nonetheless, concerns have been raised about whether the increase in flexibility might make people more vulnerable to scams. In its report on 'pension freedom guidance and advice' published in October 2015,

the Work and Pensions Select Committee recommended that the Government **"**urgently redouble its publicity efforts around pension scams." In its response in December 2015, the Government explained that it worked with the National Crime Agency, regulators and the industry to tackle scams and understand emerging threats. Its anti-scam strategy was also focussed on "improving consumer awareness, to prevent people falling victim to scams in the first place." It would also work with other bodies to consider how to ensure "reported data on pension scams is clearer, and how best to drive forward this agenda, ensuring that there is an ongoing focus on the pension freedoms in 2016."

Consumer scams

There are many different types of consumer scams. Scams can operate by post, phone call, text message or email, or even from an unsolicited visit to the person's home.

Advances in technology have enabled scammers to become increasingly sophisticated in their methods. For example, some websites or phone numbers can look like official government sites, with the result that people pay for services that they could get cheaper or for free if they used the official government service (for instance, renewing a passport or driving licence). Phishing emails and texts try to trick the consumer into giving out their personal bank details.

Although anyone can fall for a scam, vulnerable people (such as the elderly and those with mental health problems, learning difficulties or dementia) are especially susceptible and are more likely to be targeted. All scams should be reported to Trading Standards (via Citizens Advice online portal) and to Action Fraud. From time-to-time, Trading Standards teams have joined with Citizens Advice Bureaus to operate 'Scam awareness' campaigns.

1. Overview

Citizens Advice describes scams as "a scheme to con people out of their money or personal information". It adds:

> Scams aren't a minor inconvenience: they cause distress and misery, they ruin lives in some cases and, even where the losses are comparatively low, they lead to a widespread loss of consumer confidence.[1]

It runs an annual Scams Awareness Month, most recently in July 2016, which aims to raise awareness of scams, how to avoid them, and how to report them.

The annual cost of fraud against individuals – including mass marketing fraud and identity fraud – has been estimated at some £9.7 billion.[2] Research conducted in April 2015 by Age UK suggested that 53 per cent of people aged 65+ believed they have been targeted by fraudsters.[3]

Action Fraud is the UK's national reporting centre for fraud and cybercrime, and would usually be the first port of call for anyone wishing to report a suspected scam. Action Fraud also operates a specific service for those who wish to make a report on behalf of a particularly vulnerable victim: see Action Fraud website, *Vulnerable Victims and the Victims' Code* [accessed 2 September 2016].

For further general information, please see:

- Action Fraud website, *A-Z of Fraud* [accessed 2 September 2016]
- Citizens Advice website, *Stopping someone vulnerable from being scammed* [accessed 2 September 2016]
- Age UK, *Only the tip of the iceberg: Fraud against older people - Evidence review*, April 2015
- Age UK, *Policy Position Paper: Crime and scams (England and Wales)*, April 2016
- Chartered Trading Standards Institute website, *Stand Against Scams* [accessed 2 September 2016]

1 Citizens Advice, *Scams Awareness Month*, July 2016
2 Experian/PKF Littlejohn, *Annual Fraud Indicator 2016*, May 2016, p26
3 Age UK, *Only the tip of the iceberg: Fraud against older people - Evidence review*, April 2015

2. Financial and investment fraud

Scams come in many forms, and through different channels, but scams involving false investment opportunities are one of the commonest and some of the most devastating when they involve the life savings of elderly individuals.

The main 'policeman' for the retail financial services sector is the Financial Conduct Authority (FCA). The FCA derives its powers from the *Financial Services and Markets Act 2000* (FSMA) and it is this which gives it its statutory objectives:

- Securing an appropriate degree of protection for consumers
- Promoting effective competition in the interests of consumers
- Protecting and enhancing the UK financial system

'Protection of consumers' is a multi-layered activity which includes:

- The approval of who can operate in the financial services sector and offer regulated services;
- The establishment of rules and standards for everyday business;
- Consumer information/education programmes; and
- Active investigation and prosecution of unauthorised activity.

By definition it is the last of these which is of greatest application to the current debate.

2.1 FCA enforcement action[4]

The FCA takes enforcement action against unauthorised firms or individuals. Although occasionally the need for authorisation can be unclear, firms and individuals acting in breach of FSMA are likely to be scam firms and involved in some element of investment fraud. Consumers dealing with unauthorised firms will not be covered by the Financial Ombudsman Service or the Financial Services Compensation Scheme if things go wrong.

In 2015, the FCA received over 8,500 reports about potential unauthorised activity (not just pension scams). In cases of proven unauthorised activity the FCA has a range of options open to it:

- taking civil court action to stop activity and freeze assets,
- insolvency proceedings and,
- for the most serious cases, criminal prosecution.

Fraud in the financial sector is covered in Library Briefing Paper SN-06872 (April 2014).[5]

The FCA comment on the scale of their activity:

---

4 This section is an edited version of material provided directly be the FCA

5 Crimes and misdemeanours: penalties and punishment in the UK financial services sector. CBP-6872

> Last year, our actions sent 8 people to jail for a total of 32 years, we froze over £2.7 million, returned nearly £1.9 million to victims and secured injunctions and other orders against unauthorised firms and those behind them. These actions are designed to do three things: firstly, to detect and disrupt unauthorised firms and individuals; secondly, to protect other consumers from falling victim to unauthorised business activity and; thirdly, to bring justice to the victims.
>
> We also issued public warnings about 250 unauthorised firms and individuals in order to deter potential investment frauds. As our remit is limited to unauthorised business activity, we cannot take action against all types of investment fraud and, in some cases, even if we can take action, the money has already been lost. As a result, we also support a range of consumer education programs, such as ScamSmart, to build consumer awareness and increase scepticism, both healthy defences to investment fraud.[6]

Alongside enforcement and prosecution, the other important layer of anti-fraud activity is consumer awareness and education. This has largely been effected through the FCA's ScamSmart campaign.

2.2 ScamSmart Campaign

Across a broad range of outlets the FCA seek to prevent financial crime through consumer education. It tries to increase consumer awareness of investment fraud and the actions people can take to avoid it.

The ScamSmart website, www.fca.org.uk/scamsmart, gives consumers tips on how to spot the techniques used by fraudsters and hosts the FCA Warning List which is a list of firms and individuals that the FCA knows are operating without its authorisation. The web tool helps members of the public search this list, find out more about the risks associated with an investment opportunity and find out further steps they can take to avoid investment scams. The tool captures data from consumers who have been approached about their pension and signposts to Pension Wise for further advice.

According to the FCA the average amount of money lost to investment fraud per victim is an estimated £20,000. Whilst it is not possible to say how much fraud the campaign has prevented, the FCA say that

> […] since ScamSmart first launched in October 2014, we have reached over 3million at-risk consumers, over 350,000 people have visited the campaign website and more than 30,000 have checked an investment on our Warning List. From 1st April 2015 to 31st March 2016, over 4,000 consumers using the Warning List (30% of all checks) indicated that the investment they were checking involved money from their pension.[7]

2.3 Banking fraud

The main high street banks, individually and collectively, spend considerable sums not only on their own internal security and the security of, for example, online banking, but also on anti-fraud information and awareness campaigns such as the Knowfraud

6 Source: FCA August 2016
7 Source: FCA August 2016

campaign. This is targeted at ordinary individuals and highlights the different sorts of fraud that individuals might come across:

Vishing

In these cases a fraudster will say they are from the bank or police, and that a fraudulent credit card payment has been spotted or a card due to expire needs to be replaced. To convince the intended victim they are genuine, the caller will suggest the customer hangs up an1d calls the bank back on the number printed on the back of their debit or credit card. But the fraudster never actually disconnects the line so that when you call the real number you are still speaking to them.
Often the fraudster will then ask for the customer's PIN and then send a courier to the victim's home to collect the bank card, promising to provide a new one. By now the assailant has obtained the victim's name, address, bank details, card and PIN – enough to make large bogus payments.
If you have a suspicious call, if possible use another phone or wait at least two minutes for the line to disconnect before picking up and dialling again.

"Safe account"

Often criminals, posing as a bank, will instruct a customer that their account is under threat – usually from a corrupt bank employee or cyber criminals. They will be instructed by the "bank" to transfer money into a new "safe account" which is actually the fraudster's account.
Your bank will NEVER ask you to authorise the transfer of funds to a new account or hand over cash.

Test transactions

In some circumstances, criminals pretending to be from a bank might email a customer asking you to perform a "test" transaction online, sometimes claiming there is some technical issue on their account.

Your bank will NEVER ask you to carry out a test transaction online.

Courier fraud

Often a follow-up to vishing (see previous), having posed on the phone as a fake bank employee to extract key security information – such as a customer's full PIN code – the criminal my also say that they are sending an official courier to their home to collect the corresponding card. These couriers will have "official" identification.

Another courier fraud ruse is for the criminal to pose as the bank in order to ask the victim to participate in a fake police investigation, usually involving a corrupt bank employee who has been stealing from customer accounts. Typically the customer will be asked to withdraw substantial sums of money over the counter at their bank without arousing the suspicion of the staff. They are then told to wait at home for it to be collected by a courier for safe keeping.

Your bank will NEVER send someone to your home to collect cash, bank cards or anything else. [8]

[8] BBA Press Release 13 October 2014

3. Pensions

Changes in the law in April 2015 gave people aged 55 and over more flexibility over when and how to draw their defined contribution pension savings.[9] They can now:

- Take their pension savings as cash (in one lump sum or a series of smaller amounts over time);
- Buy an annuity (or other income-generating product);
- Use a drawdown pension arrangement (where they can make withdrawals from their pension pot while leaving the rest invested); or
- Any combination of the above.

The Government said it recognised that people would need help navigating the expanded range of options and therefore introduced a guidance service – Pension Wise.[10] Nonetheless, concerns have been raised about whether the increase in flexibility might make people more vulnerable to 'scams'.[11]

The Pensions Advisory Service (TPAS) explains that people can become the target for illegal activities, scams or inappropriate and high risk investments:

> It's good to remember that pension scams can take many forms and usually appear to most, to be a legitimate investment opportunity. But, pension scammers are clever and know all the tricks to get you to hand over your savings. They target anyone and everyone, pressuring you into transferring your pension savings, often into a single investment.
>
> The investments are normally overseas, where you have no consumer protection, and typically promise you a high guaranteed rate of return (typically 7 or 8% or higher). These are often false investments in luxury products, property, environmental solutions or storage and parking, which often don't exist or are extremely high risk with low returns.[12]

It explains the potential consequences for individuals:

> If you transfer your pension savings into a scam, you run the very real risk of losing a significant, if not all of your pension savings, as well as facing high commission or arrangement fees.
>
> Additionally, accessing your pension early is only allowed in very special circumstances, such as ill health. If you access and transfer your pension before the age of 55, you will this will classify as an 'unauthorised payment' from your pension fund. This will result in significant tax penalties and HMRC can impose a charge of up to 55% of the value of your pension.

---

9 *Taxation of Pensions Act 2014*; See Library Briefing Paper SN-06891 Pension flexibilities (May 2016)
10 *Pension Schemes Act 2015*, s47
11 HL Deb 18 June 2015 c1261
12 TPAS website – common concerns – pension scams

> This means that at the end of the transaction you may just get little or nothing of your original investment back, and also owe money to HMRC.[13]

It has also produced a flow chart showing the stages of a scam.

In evidence to the Work and Pensions Committee in September 2015, Citizens Advice said that since the introduction of the pension freedoms in April, it had seen more consumers, particularly those over 55, becoming repeat targets of scams. Examples were people being asked by fraudsters to give access to their pension pots, promises of high rates of return though options to invest abroad etc.[14]

The FCA said that while the total number of scams had not necessarily gone up, it did think that people with pension savings did were becoming an "attractive target to scammers."[15]

The Work and Pensions Committee recommended that the Government redouble its efforts:

> 24. The pension freedom reforms have increased the prospects of people being conned out of their life savings. Financial scammers are notoriously adept at reinventing themselves to take advantage of such opportunities. But this does not mean scams should be accepted as a fact of life. The Government and the FCA are taking the right approach in promoting awareness as the best weapon against scamming. But they could do more. In particular, pension providers are an underused point of contact, for example when a customer wishes to withdraw funds to invest in a suspicious scheme.
>
> **25. *We recommend the Government urgently redouble its publicity efforts around pension scams. We further recommend the FCA tighten its scam awareness and reporting requirements for regulated firms.*[16]**

3.1 The Government's approach

In December 2015, in response to the Work and Pensions Committee's recommendation, the Government set out its approach to tackling pension scams:

> 2.8 The government takes the issue of pension scams very seriously and works closely with the National Crime Agency (NCA), regulators, industry and others via Project Bloom, the multi-agency task force led by the NCA, to tackle pension scams and understand any emerging threats. Project Bloom ensures a co-ordinated approach to disrupting scams by ensuring that the key departments and agencies that deal with scams are joined up and communicating with one another.
>
> 2.9 The government's anti-scam strategy is also focused on improving consumer awareness, to prevent people falling victim to scams in the first place. Raising awareness of the warning signs

---

13 TPAS – what happens if I transfer into a scam

14 Oral evidence: Pensions freedom guidance and advice, HC371, 7 September 2015, Q14-15

15 Oral evidence: Pension freedom guidance and advice, 16 September 2015, Q70 and 74

16 Work and Pensions Committee, Pension freedom guidance and advice, First report 2015-16, HC 371, October 2015 para 25

> and sources of reputable guidance and advice is a useful defence against the lure of scammers who often appear convincing.
>
> 2.10 The regulators, the FCA and The Pensions Regulator (TPR), are both running consumer awareness campaigns to mitigate the risk of pension scams. The FCA run a campaign around investment scams called ScamSmart, and provide an online tool that allows consumers to assess the likely validity of a potential investment. The FCA also signposts consumers to reputable sources of advice. TPR runs the Scorpion campaign, which includes videos, action packs, leaflets and guidance, to help raise awareness amongst trustees, business advisers and individuals of the threats posed by scams. These campaigns, with core messages such as avoiding cold-callers, are ensuring that consumers accessing the freedoms have the information they need to protect themselves from scams.
>
> 2.11 Pension Wise also specifically alerts its users to potential scams during appointments and the Pension Wise website and summary document that users receive following their appointment contain guidance on avoiding scams. Pension Wise also makes it clear through advertising and their website that no cold calls are ever made by its guiders.
>
> 2.12 The government agrees with the committee that scammers must be stopped and will consider what steps it can take to ensure that the wider impact of the pension reforms on scams is fully understood. For example, at present those who fall victim to scams after having accessed their pension under the freedoms are classified as victims of investment fraud, rather than pension fraud. The government will therefore work with Action Fraud and the National Fraud Intelligence Bureau, through Project Bloom, to consider how to ensure reported data on pension scams is clearer, and how best to drive forward this agenda, ensuring that there is an ongoing focus on the pension freedoms in 2016.
>
> 2.13 The government, the regulators and the industry are there to help, but people need to be on their guard too against cold callers, offers of unrealistic investment returns, promises of tax loopholes or other dubious advice linked to their pension pot or cash lump sums. As with any important financial decision, people should seek reputable guidance and independent financial advice to support them to make a decision on how to use their pension savings when they come to retire.[17]

Since then, the Government has announced changes aimed at making the provision of public pensions guidance more effective and increasing access to advice. This includes plans for a new pensions guidance service, bring together pensions guidance currently provided by three different bodies and "charged with making sure that consumers can get all their pensions questions answered in one place."[18] Provision for the new body is to be included in the forthcoming Pensions Bill. In addition, on 30 August 2016, it launched a consultation on a pensions advice allowance. For more detail, see Library Briefing Paper SN-07042 Pension Wise: the guidance guarantee (August 2016).

---

17 HM Treasury, Pension freedom guidance and advice: government response to the Work and Pensions Committee's first report of session 2015-16, Cm 9183, December 2015; HC Deb 17 November 2015 c135WH

18 HM Treasury, Public financial guidance review: proposal for consultation, March 2016

3.2 Advice from the regulators

Both regulators – the Financial Conduct Authority (FCA) for personal pension schemes and the Pensions Regulator (TPR) for work-based pension schemes – have been working to raise awareness.

The FCA warns people to be wary if they are cold-called with the offer of a "free pensions review" and encouraged to move their pension to "get better returns" or release cash sums:

> If you get cold-called, the safest thing to do is to hang up, as chances are the investment is very risky or a scam. If you get these offers via email, text or online adverts, it's best to simply ignore them.
>
> 'Free reviews' offered out of the blue are designed to persuade you to move money saved in your existing pension pot to a high-risk scheme.
>
> Your pension pot is then typically invested in unusual investments such as overseas property, forestry, storage units, care homes, biofuels or businesses you may not be familiar with. You may be promised guaranteed returns and/or a cash sum from your pension to tempt you to take up these offers.
>
> Professional financial advisers offering advice that is impartial and in your best interests are very unlikely to cold call you offering their services. Professional advice on pensions is not free.
>
> **The risks**
>
> 1. Some of these investments are badly run, while others may be outright scams. As they are promoted as long-term pension investments, several years could go by before you realise something is wrong
> 2. Where cash sums are released, you may have unexpected tax charges to pay, up to 55% of your payment. Find out more about pension unlocking
> 3. You could lose some or all of your pension pot. While these investments may offer higher rates of potential returns, the returns are not guaranteed and the money you invest is at risk
> 4. Unusual investments tend to be unregulated and high risk, and may be difficult to sell if you need access to your money
> 5. Most of the companies making these offers are not authorised or regulated by the FCA. This means you may have no right to complain to the Financial Ombudsman Service (link is external) or to claim compensation from the Financial Services Compensation Scheme (link is external) if things go wrong.[19]

It directs people to sources of information, financial advice or the guidance service set up to support the pension freedoms, Pension Wise.[20] It has produced a leaflet Protect your pension pot.

TPR has also issued guidance for business advisers, trustees and individuals: Pension scams. The ten steps it says people should take to protect themselves are:

---

19 FCA, Pensions and retirement income (last updated 30 June 2016)
20 Ibid

1. Be wary of cold calls and unsolicited texts or emails

Scammers will often claim they're from Pension Wise or other government-backed bodies. These organisations would never phone or text to offer a pension review.

2. Check everything for yourself

People have fallen for scams because they'd been 'recommended by a friend'. Do your homework, even if you consider yourself to be financially savvy – false confidence can lead to getting stung.

3. Make sure your advisers is on the Financial Conduct Authority approved register

Pensions scammers may pose as financial advisers. Check to make sure yours is registered on the FCA website.

4. Check the FCA's list of known scams

Visit the FCA's scamsmart to see if the deal you're being offered is a known scam.

5. Steer clear of overseas investment deals

Well-known scams include unregulated investment in a hotel, vineyard or other overseas opportunities, and where your money is all in one place – and therefore more at risk.

6. Don't fall for guaranteed returns of professional looking websites or brochures

You can never guarantee returns on an investment, and anyone can create a smart website or brochure these days. Question everything, however credible it sounds or looks.

7. Don't be rushed into a decision

Scammers will try to pressure you with 'time limited offers' or send a courier to your door to wait while you sign documents. Take your time to make all the checks you need - even if this means turning down an 'amazing' deal.

8. If you're aged 50 or over and have a DC pension, talk to Pension Wise

Pension Wise is there to help you investigate your retirement options. Visit the Pension Wise website for more information (and to check what kind of pension you have).

9. Ask The Pensions Advisory Service for help if you have doubts

You can call them on 0300 123 1047 or visit the TPAS website for free pensions advice and information.

10. Contact your provider and call Action Fraud if you've already signed and think you've been scammed

If you've already signed something you're now unsure about, call Action Fraud on 0300 123 2040 and contact your pension provider immediately. They may be able to stop a transfer that hasn't taken place yet.[21]

---

[21] TPR website, Protect yourself against pension scams

4. Consumer scams

4.1 Why people can be vulnerable to consumer scams

Consumer scams are schemes designed to 'con' people out of their money. According to the consumer body Which?, fraud is now at record levels, with more than 5 million scams costing Britain £9 billion each year.[22]

There are many different types of scams and fraudsters have become increasingly sophisticated in the methods they adopt. Scams can operate by post, phone call, text message or email, or even from an unsolicited visit to the person's home. In terms of spotting consumer scams, Citizens Advice suggest that a scammer may:

- contact a consumer out of the blue
- make promises that sound too good to be true
- ask the consumer to pay for something up-front (for example, they'll ask him/her to pay a fee before a prize can be claimed)
- ask the consumer to make a quick decision by saying things like 'if you don't act now you'll miss out'; this puts the consumer under pressure and doesn't give them time to think
- be over-familiar and over-friendly with the consumer
- tell the consumer that an offer has to be kept secret
- ask the consumer for their bank account details
- give a mobile number or PO Box number as the contact for their company (these are difficult to trace and may be a sign that the company doesn't exist or isn't legitimate)

Consumers of all ages can be the victim of a scam. As Citizens Advice points out, it is often thought that older people are the most likely to fall for scams, but while this does happen, other age groups can be just as likely to be taken in:

> If you're aged between 35 and 45, you can be caught out by too-good-to-be-true offers and get-rich-quick schemes, especially if you've suffered a difficult situation such as a job loss. For example, there are training scams which affect people who are hoping to improve their employment chances but which will defraud you of all your money instead.
>
> […] People are often embarrassed to admit they have fallen for a scam or simply refuse to believe they have been conned.[23]

Although anyone can fall for a scam, vulnerable people are more likely to be targeted. Older people and people with mental health problems, learning difficulties or dementia are especially vulnerable to scams.

---

22 "Join our campaign and help us reach 150,000 signatures," Which?, [online] (accessed 6 September 2016

23 "How to spot a scam", Citizens Advice website, [online] (accessed 6 September 2016)

4.2 Types of consumer scams

Often, it is not easy to identify a scam, particularly if 'phishing emails' are used. Phishing emails try to trick the consumer into giving out personal information (such as bank details). Examples of 'phishing emails' identified by 'Which?' include:

- Lottery scams, which claim that the consumer has won a fantastic prize, usually money, in a public ballot. To claim the prize, the consumer must first pay some kind of fee or provide their bank details. Of course, there is no prize.
- Government scams, whereby fraudsters send convincing emails that pretend to be from a trusted agency. It is not unusual for phishing emails to cite government organisations, such as the Financial Conduct Authority or HM Revenue and Customs, in order to make the email appear more convincing. The emails ask the consumer to provide their bank details (either by email or by clicking on a link).
- Security scams, which usually involves an unsolicited phone call supposedly from a 'security expert' offering to fix a person's PC or people are deceived into believing they are speaking to their bank.

4.3 Three case studies

Fake lotteries

The vulnerable are particularly susceptible to lottery or sweepstake scams, often originating from abroad (Spanish, Canadian and Australian lottery scams are among the most common). With such scams fraudsters usually notify the recipient by letter that they have won a large sum of money in an international prize draw. So that the payment can be processed, the recipient is advised to pay an 'administration fee' and/or supply personal information (such as bank details) and copies of official documents (such as their passport) as proof of identity. Of course, there is no prize and the fraudsters are able to use this information not only to steal the victim's money but also their identity.

In respect of unsolicited mail originating from within the UK, the Government has already taken steps to make sure there are preference services in place for those customers who do not want to receive it. The Direct Marketing Association currently run two separate 'opt out' services: the Mailing Preference Service (MPS) will stop addressed mail and the 'Your Choice' preference service should stop unaddressed mail. Royal Mail also runs its own door-to-door 'opt-out' scheme to stop unaddressed mailings delivered by Royal Mail.

In respect of unsolicited mail originating from outside the UK, Action Fraud provides consumers with the following advice:

- Protect yourself against lottery fraud
- Never respond to any such communication. If you haven't entered a lottery then you can't have won it.
- Official lotteries in other countries operate in much the same way as the UK's National Lotto. No official lotteries that we know of contact people to tell them of their win.

- We don't know of any official lottery operators who ask for fees to collect winnings. Any request for a fee payment is a good indication that someone is trying to defraud you.
- Never, ever disclose your bank details or pay fees in advance.
- If they've provided an email address to respond to, be very suspicious of addresses such as @hotmail.com or @yahoo.com or numbers beginning with 07 because these are free to get hold of.
- Genuine lotteries thrive on publicity. If they ask you to keep your win a secret it's likely to be a fraud.
- Many fraudulent lotteries have bad spelling and grammar – see this as a warning that fraudsters are at work.

If a person (or vulnerable relative or friend) has been the victim of a lottery scam, the matter should be reported immediately to the police via the Action Fraud website. In addition, Action Fraud provides the following advice:

- If you have responded to the email/letter, break off all contact with the fraudsters at once.
- If you have given the fraudsters your bank account details, alert your bank immediately.
- Be aware that you're now likely to be a target for other frauds. Fraudsters often share details about people they have successfully targeted or approached, using different identities to commit further frauds.
- People who have already fallen victim to fraudsters are particularly vulnerable to 'recovery fraud'. This is when fraudsters contact people who have already lost money through fraud and claim to be law enforcement officers or lawyers. They advise the victim that they can help them recover their lost money – but request a fee.

Copycat websites

Searching on the internet in order to apply for a European Health Card (EHIC), book a driving theory test or renew a passport, brings up websites for businesses which offer to check, review and forward applications for a fee. Advertisements for these businesses may feature prominently in search results.

In recent years, consumers have complained about private companies that set up websites deliberately designed to look like official Government sites and then charge people for services that are available directly from the Government either at no cost or for a much lower fee. It is not unlawful to provide reviewing and forwarding services, but businesses should make it clear on their websites that they are not affiliated to the Government and that consumers will be paying for a service which they could obtain from Government for free or at a lower cost. Unfair and misleading practices are prohibited by the *Consumer Protection from Unfair Trading Regulations 2008* (CPRs). The Regulations are enforceable by Trading Standards through the civil and criminal court. The Chartered Trading Standards Institute (CTSI) has published guidance notes for members of the public called *"Wise up to the web – avoid being conned by deceptive websites"*.

In March 2014, the National Trading Standard Board (NTSB) welcomed additional funding of £120,000 (for this financial year) to investigate

copycat websites. In the March 2015 Budget, George Osborne, then Chancellor of the Exchequer, said the government would give the National Trading Standards Board an extra £250,000 to help it crack down on copycat websites masquerading as legitimate government services.

In certain circumstances, the Advertising Standards Authority (ASA) will investigate misleading websites that have been brought to its attention by members of the public. In brief, the content of advertising, sales promotions and direct marketing across all media in the UK is self-regulated by the ASA. It does this by enforcing the Advertising Codes. The overarching principle is that advertisements are expected *to be legal, decent, honest and truthful.*

The ASA has received a number of complaints about firms that pose as official websites. Typical concerns are:

- It's unclear from the website whether they're an official service
- The company has appeared above the official body on Google search results
- Copycat sites charge fees for services that could have otherwise been free or cheaper
- The consumer did not realise until after the transaction that they would have to pay a handling fee in addition to paying for the service.

The ASA can take action against misleading advertisements and has various sanctions at its disposal, including:

- a name and shame section on its website,
- 'ad alerts' advising CAP members to withhold advertising space, and
- methods for seeking the removal of a companies' paid for search advertisements

In respect of wider trading practices, for example, where a company is charging consumers extortionate prices for false services, complaints should be made to local authority Trading Standards.

Cold calling scams

Cold calling generally involves a high pressure salesman or other representative making an unsolicited visit to a consumer's home in an attempt to sell goods or services. Alternatively, bogus callers may pretend to be officials (such as HMRC officials) in order to encourage a person to provide bank account details or other valuable personal information.

For all doorstep sales made on, or after, 13 June 2014, the new Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 apply, replacing the Doorstep Selling Regulations. Under the new Regulations, the cancellation period for doorstep sales has been extended to 14 calendar days after delivery of the goods. For service contracts the cancellation period is 14 calendar days after the contract has been entered into. However, there are exceptions,

including perishable items such as food and drink, and personalised items.

A further development has been the introduction of 'No Cold Calling Zones' in various parts of the country. A 'No Cold Calling Zone' is a designated area where the resident community declare they no longer wish to accept traders calling at their homes without an appointment. Such zones are supported actively by Trading Standards.

The first pilot zone was launched in Cranbrook, Tunbridge Wells in 2006 by Tunbridge Wells Community Safety Partnership. There are now many hundreds of No Cold Calling Zones nationally and more planned. For example, there are zones operating in Luton, Lincoln, Hampshire, Kent, Nottingham, Enfield and Norfolk. No Cold Calling Zones are viewed as a community safety initiative which aims to reduce the likelihood of residents, particularly old and vulnerable people, becoming victims of rogue traders and distraction burglaries.

A zone is designated via the installation of signs at the entrance and exit to the zone and residents are supplied with educational and advice information and door stickers. Residents are also given telephone numbers to ring if they are concerned about anyone knocking on doors in the neighbourhood. Trading Standards Officers and/or the police will usually respond to the call and, where appropriate, can demand to see identification. In order to inform legitimate callers, letters are usually sent to interested parties such as utility companies explaining the scheme. For legitimate callers, the scheme simply reinforces good practice and they will not be prevented from doing their work.

Guidelines on setting up a No Cold Calling Zone have been published by the Chartered Trading Standards Institute (CTSI). Various local authorities also provide information on setting up zones on their websites.

Although not scams, nuisance phone calls (i.e. unsolicited and unwanted marketing messages, silent or abandoned calls) and spam texts cause widespread harm and inconvenience especially to the vulnerable, as acknowledged by previous and current Governments and the relevant regulators – Ofcom (the communications regulator) and the Information Commissioner's Office (ICO).

Ofcom deals with silent calls while the ICO deals with marketing calls. As well as Ofcom and the ICO, the Telephone Preference Service (TPS) and Silent CallGuard offer advice and assistance. If a person is concerned about unwanted marketing calls, he/she can register their phone number with the TPS. There are also other options, including call-blocking technology, available.

Detailed information on recent government action and regulators' enforcement action is available in a separate Commons briefing paper "Nuisance calls: unsolicited sales and marketing, and silent calls", (SN06033) dated 24 June 2016.

4.4 What people can do to protect themselves?

Reporting a scam

To report a scam, a consumer should call the Citizens Advice Consumer Helpline on 08454 040506 or they can use the online enquiry form. If appropriate, Citizens Advice may refer the case on to Trading Standards and action may be taken against a rogue trader.

If a consumer suspects that a fraud has been committed, a consumer can report the matter to Action Fraud via their online reporting tool.

If a consumer suspects that a website may be selling counterfeit goods, they can report the matter to Brand-i. This alert will be forwarded on to the brand-holder's protection department. Brand-i is a directory website in partnership with the Trading Standards Institute, which provides a list of all the online shops selling genuine branded products.

The consumer body Which? has started an online petition urging the government to take further action to ensure companies safeguard all consumers from scams.

Getting their money back?

Consumers who have been scammed do not always get their money back, especially if they have parted with cash or made a bank transfer or if the company is based abroad. If a consumer has responded to an email from a fraudster and sent money, there is no automatic mechanism to get their money back if it's a transaction they have authorised. Proper legal advice should be sought from Citizens Advice or Trading Standards.

If the consumer has bought goods or services using a credit or debit card they may be able to pursue the following options:

- Under section 75 of the Consumer Credit Act 1974 (as amended), a credit card company is jointly and severally liable for any breach of contract or misrepresentation by the trader. However, for section 75 to apply the good or service bought by the consumer must have cost over £100 and not more than £30,000. By way of example, section 75 might be useful where goods or services never materialise and the trader has disappeared.
- Chargeback – if a consumer has bought a good or service with a debit card, they may be able to ask their card provider to reverse the transaction using chargeback. The chargeback scheme applies to all debit card transactions including goods costing less than £100, although exact rules may vary between the various networks. It is important to note that chargeback is not enshrined in law but is part of Scheme Rules, which participating banks subscribe to.
- Unauthorised transactions – if an unauthorised transaction has been made on a consumer's card then they may be able to recover the money from their bank. The Payment Services Regulations 2009 and the Banking Conduct of Business rules

place obligations on banks and building societies to provide a refund in certain circumstances.

4.5 What action is being taken by the regulators to raise awareness

From time-to-time, Trading Standards teams have joined with Citizens Advice Bureaus to operate 'Scam awareness' campaigns. The aim being to increase awareness of scams and to provide consumers with practical advice on how to avoid being scammed. For instance, to combat scams, Trading Standards promote the following tips:

- Stop, think and be sceptical. If something sounds too good to be true it probably is.
- Do not be rushed into sending off money to someone you do not know, however plausible they might sound and even where an approach is personalised.
- Ask yourself how likely it is that you have been especially chosen for this offer – thousands of other people will probably have received the same offer.
- Think about how much money you could lose from relying to a potential scam – it's not a gamble worth taking.
- If you are unsure of an offer, speak to family or friends and seek advice from Citizens Advice before sending any money or giving out any banking or credit card details.

In addition, the Action Fraud website highlights the latest scams based on reports from the public.

BRIEFING PAPER
Number CBP-07691
6 September 2016

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer