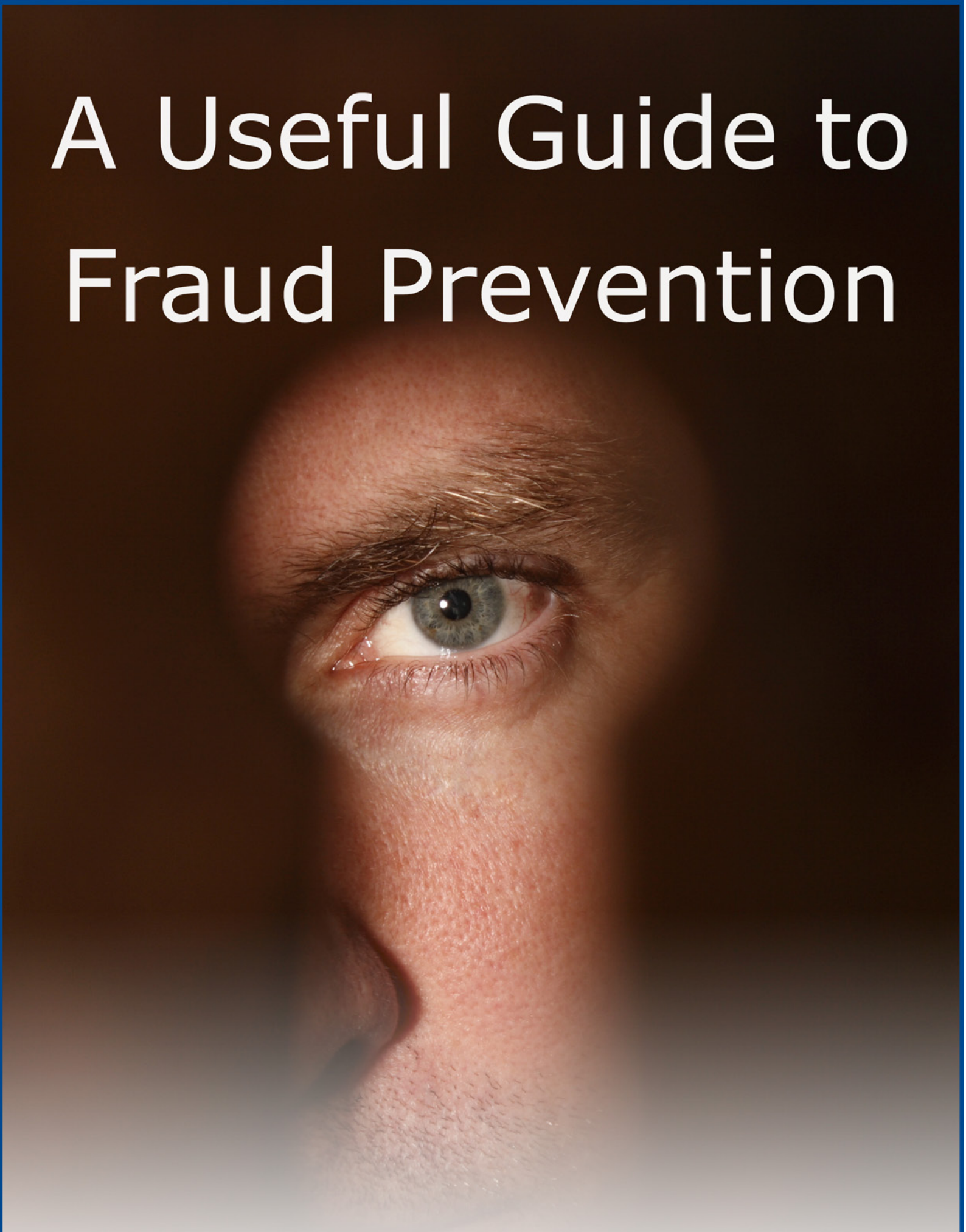
A Useful Guide to Fraud Prevention



Janet Hope

ISBN 978-1-906460-23-5

Pansophix

Pansophix

A Useful Guide to Fraud Prevention

Published by Pansophix Online
22 Torquay Road, Chelmsford,
Essex, CM1 6NF, England

Written by Janet Hope

This edition published April 2010 (a)

ISBN 978-1-906460-23-5

CONTENTS

This Useful Guide contains several checklists and a Risk Assessment Grid which can be downloaded as a separate PDF file. This file can then be printed out or emailed to friends or relative you feel would benefit. You can download this file from here.

1 Introduction

The issue of fraud is pervasive at the individual citizen level and also at the business, large organisation, level. The chances of it happening are not confined to a certain type of person or a specific commercial sector. Nor is it bound by geography and so any person and any organisation almost anywhere can be vulnerable to the one-off or persistent fraudster, minded to take advantage when an opportunity presents itself.

Costing the United Kingdom economy at least £13.9 billion a year, affecting people, corporations and smaller business alike, the threat requires both macro and micro management. Perhaps the biggest consequence at the micro level is the need for individuals to take greater responsibility for their physical safety and for the security of their money, property and personal data.

The notion that fraud is a victimless crime is long gone with more and more people worried about having their identity stolen, scams of one kind or another, the miss-use and loss of personal data, and the sophisticated types of financial crime reported in the media on what seems to be an almost daily basis.

The domino effect of these and other frauds is that more and more ordinary people are having their lives impacted by frauds. Incidents range from telephone and doorstep cold calling so as to dupe and steal, through to corruption at corporate and political levels resulting in large scale deception and theft.

The unnerving thing is that many of the frauds are committed by people the individual either knows or is tricked into trusting. For reasons of embarrassment, the fear of looking foolish or worse still having been threatened in some way, it is believed that many such crimes go unreported.

In the same way it is likely that the possible damage to reputation probably accounts for a general reluctance on the part of employers to punish employees whom they find committing fraud or involved in some sort of wrongdoing.

In broad terms it's as though we are not yet ready to face up to the fact that we are not infallible. Getting it wrong is one thing, being unaware is fine up to a point but not being bothered about our exposure to fraud is, in this day and age, downright stupid.

This Useful Guide aims to drive forward the message on fraud and fraud prevention. It focuses on the elderly and retired who, as a group, present an easy target to fraudsters and doorstep scammers.

The practical hints and tips are not exclusive to the elderly and retired for many can be applied equally to the family and wider domestic situation.

Background interest

The study of fraud dates back to the mid-twentieth century although where it belongs as an academic discipline has tended to be driven by the purpose of the research and the motives of those conducting it.

Thus it is that much of the writing about fraud has been sociological, criminological or socio-criminal in nature. We also have the products of investigative journalism and public audits to inform us of fraud and wrongdoing, particularly in regards to the corruption associated with commercial and public bodies.

It needs to be understood that prior to the Fraud Act 2006 English law did not define fraud. The central issues have historically been the elements of deception and deprival,

> "to defraud is to deprive by deceit" Huntington I and others. 1996: p3

As with other criminal acts there is a perpetrator and a victim but because they do not always have to meet, know each other or have direct contact, fraud has become in the minds of many an invisible crime. In relative terms it is easier to see the use of guns, knives, threats and violence as crime but less easy to accept that the genial and matey doorstep caller, or the person at work who is submitting false expenses claims are, in real terms, just as much the criminal.

The problem of fraud falls under the banner of economic crime and includes ...

- Telemarketing
- Door to door sales
- Mail orders
- Internet shopping
- Home repairs and construction
- Buying and servicing vehicles
- Financial transactions
- Bounced cheques
- Credit card problems
- Illegal money and property transfers
- Pensions scams
- Mismanagement of accounts, funds, assets.

The concept of fraud has actually been around since the time of Henry Chaucer. While not referred to as such in Chaucer's The Pardoner's Tale there appears to be a sermon about greed. Modern day attempts to analyse what makes a fraudster speak of a 'Greed – Need continuum'. Certainly it appears that most

fraudsters are driven by the desire to have more of something, for example, money, simply because that is what they want, or are driven by the need to get for example, revenge on an employer, because they think they have been wronged in some way and want retribution.

However they choose to rationalise their actions the bottom line is still the same, they have intentionally set out to take something from someone or an organisation or have set out to cause a loss to someone or to an organisation.

Years ago traders who were caught interfering with foodstuffs and weigh scales were subjected to the public ridicule of the stocks or even banished from the town.

Whilst we have not as yet reverted to such measures it may be helpful to know a little more about the legal support that currently exists to tackle this growing problem.

The Legal Position on Fraud

Rosalind Wright of the Fraud Advisory Panel expressed the following personal viewpoint in her paper entitled 'Developing effective tools to manage the risk of damage caused by economically motivated crime fraud' when she said ...

> "Fraud has to be taken seriously. It facilitates other crime, such as terrorism. The response from law enforcement world-wide has not been sufficient."

Law enforcement in the UK deserves to be differentiated from any broad contrasts that can be made between different countries by virtue of the commissioning, by the Association of Chief Police Officers (ACPO), of a special report aimed at establishing the true cost of fraud in the UK. Compiled by Morgan Harris Burrows LLP in association with Professor Michael Levi, fraud has been found to be costing the UK economy at least £13.9 billion a year.

As recently as March 2007 the ACPO report was presented at a parliamentary breakfast with the then Attorney General, Lord Goldsmith in attendance. The findings in this latest report addressed the growing frustration at the lack of a truly reliable figure for the impact of fraud on the UK economy.

As a myriad of offences, sanctioned by a complex criminal justice system and detailed fabric of civil law, dealt with by a plethora of agencies in both public and private sectors, each with varying powers and practices, fraud had until this time been a confusing area to get to grips with and somewhat neglected as a result.

It is interesting to note that the review was minded that government ought to take a more concerted stance towards protecting consumers and businesses from fraud. It is important to mention here that the review believed that government ought to ensure that law enforcement, alongside regulations and the Criminal Justice System, should expressly prevent, deter, detect, investigate and punish fraud. It is assumed this was a direct reference to the Fraud Act and desire that police area commands give fraud a higher priority.

Another aspect of this review applicable at both macro and micro levels to businesses and private citizens is the recommendation for a National Fraud Reporting Centre. This led to the development of the National Fraud Strategic Authority (NFSA), an Executive agency of the Attorney General's Office.

The NFSA was set up in October 2008 with the remit to bring together the work of the various counter fraud agencies in both public and private sectors of the economy. The idea being that because fraud is not currently a national priority

for the police, it is probable that individuals and firms do not report incidents for fear nothing will be done and so there is likely to be an undisclosed amount of fraud being perpetrated. If there was a designated support centre for individuals and businesses to report incidents it would drive through this negativity and perhaps begin to reshape public awareness and concern about fraud, helping to create what the review described as **a much more fraud aware than fraud prone culture.**

With more robust statistics law enforcement would be able to develop a strategic response on more holistic lines, and as a result make combating fraud and punishing offenders much more achievable than the current disparate reporting and investigating arrangements allow.

At the very least the establishment of a national centre would arguably give individuals and businesses a place to lodge their suspicions. In turn this could possibly provide a credible means for stopping the activity that in the absence of any such body to report to, feeds a denial that there is a problem or a risk to be faced.

This then turns attention to the role of government and the mechanisms and instruments it makes available to deal with fraud as a crime. An extremely welcome piece of legislation, if for no reason beyond creating an actual offence of 'Fraud', is the Fraud Act 2006. Receiving Royal Assent on 8th November 2006 it came into effect on 15th January 2007 creating a new general offence of fraud, replacing many of the old deception offences. The Act establishes a new Section 1 general offence of fraud with three ways of committing ...

- Fraud by false representation (section 2): lying about something by whatever means, such as words or running a fake website.
- Fraud by failing to disclose information (section 3): not disclosing something when there is a legal duty to do so, such as not declaring something on a tax return.
- Fraud by abuse of position (section 4): abuse of the implied trust expected of the position, for example, employees disclosing client and customer information to an unauthorised third party.

The key point to understand is that there are two basic requirements that must be met, namely ...

- The behaviour of the defendant must be dishonest
- It must also be their intention to make a gain or cause a loss to another.

In simple terms this means it will no longer be necessary to prove that a person has been deceived. Significantly this piece of legislation clearly puts the focus on the dishonest behaviour of the suspect, and their intent on making a gain or causing a loss.

The Act also creates new offences of ...

1. Possession of articles intended for use in fraud (section 6): applies anywhere and includes any such article be it a cloned credit card, particular software or item of electronic data.
2. Making or supplying articles for use in fraud (section 7): know that it will or intend for the article to be used to facilitate or commit fraud.
3. Fraudulent business carried out by a sole trader (section 9): applies to individuals, partnerships and trusts.
4. Obtaining services dishonestly (section 11): using a stolen credit card for example.

Certainly, on the face of it, this appears to be a super legislative tool cutting through the veritable minefield which existed before when investigators, prosecutors and juries had to navigate sections of the Theft Acts of 1968 and 1978, the Companies Act of 1985, the Criminal Justice Act 1987 and the Forgery and Counterfeiting Act 1971 to mention just a few.

By simplifying the law relating to fraud with this new Act, in association with the Proceeds of Crime Act, a much easier means exists to investigate, prosecute and punish fraudsters as well as enhance the recovery of monies and assets.

If you are interested in what the law actually says read on, **otherwise go straight to the Summary**

To illustrate how this legislation defines fraud and simplifies the offence, the following is taken from the Act itself; the intention being to show the clarity of language and absence of ambiguity.

First of all is the matter of false representation.

A person is in breach of this section if he ...

- Dishonestly makes a false representation, and
- Intends, by making the representation ...
  - to make a gain for himself or another, or
  - to cause loss to another or to expose another to a risk of loss.

A representation is false if ...

- It is untrue or misleading, and
- The person making it knows that it is, or might be, untrue or misleading.

“Representation” means any representation as to fact or law, including a representation as to the state of mind of ...

- The person making the representation, or
- Any other person.

A representation may be express or implied.

A salient point to note is that it now makes no difference if the representation is made to a machine or to a person.

Next is the matter of failing to disclose information.

A person is in breach of this section if he ...

- Dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
- Intends by failing to disclose the information ...
  - to make a gain for himself or another, or
  - to cause loss to another or to expose another to a risk of loss.

Followed by the matter of fraud by abuse of position.

A person is in breach of this section if he ...

- occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
- dishonestly abuses his position, and
- intends, by means of the abuse of that position ...
  - to make a gain for himself or another, or
  - to cause loss to another or to expose another to a risk of loss.

A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

Summary

It needs to be appreciated that fraud embraces a wide variety of misleading and deceptive practices, some of which can be very complex in nature and span several years of activity. It takes an average of 5 years to investigate frauds and process cases through the courts. In time therefore it is expected that actual numbers of prosecutions will be more easily available than at present.

Cases like the Darwins from Hartlepool and Mr Madoff in America (see the detail in the "Additional Reading" Section at the end of this Useful Guide) show how important it has become for each and every one of us to show more respect for the fact that fraud is on the increase. Greed and opportunity are a toxic combination wreaking havoc for the victims of fraudsters. We have to be more alert and embark on a proactive programme of protecting ourselves as much as is reasonably practicable, from the dishonest activities of people whose intention it is to deprive or deceive.

The Fraud Review 2006 discussed a number of ways in which anti-fraud measures could be made more effective.

The Fraud Act 2006 creates an actual offence of Fraud, making the law much simpler for prosecutors to use, and for juries and organisations to understand.

The legislation has been warmly received by investigators and the police.

The threat fraud poses to the UK economy and society is now reliably pitched to be at least £13.9 billion annually.

2 Older Groups considered as "Easy Prey"

The nature of their activities and social interactions to an extent shields older people from a high level of crime victimisation compared to other groups in society. That said, however, their exposure to certain types of crime is significant given that they are less likely than other groups to defend themselves or challenge and obstruct a perpetrator.

It needs to be understood that those who commit crimes against the elderly do so because they have no compunction regarding the distress and fear they inflict on their victims.

Research conducted by Brian Steele, a Detective Chief Superintendent in the West Yorkshire Police, found that offenders saw their crime as trade. He found that they took pride in their abilities to manipulate the thoughts and fears of the elderly and prey on their mental and physical frailty.

By the same token those who peddle telephone, mail and internet scams with the lure of fantastic sums of money in lotteries, inheritances and fake investments do so knowing that the vulnerable, in particular the elderly, will be less likely to have the faculties to see it for what it is, which is **TOO GOOD TO BE TRUE!**

> If something looks too good to be true it usually is. The trouble comes when a person, who is in a situation of desperation, is more likely to hope the offer is genuine. Trouble can also arise when the person is not as astute mentally as they used to be. Indeed it may just be that the visitor, letter or telephone call comes at a time of temporary fallibility, for we can all be caught off guard.

Wherever there is a willingness to believe, the risk of becoming a victim is high.

Unfortunately there are people who are professional victimisers. That is to say they make their way in the world by deception, duplicity and general deviant behaviour. Aside from the opportunist such as one who helps an old person seen struggling with their bags only long enough to relieve them of their purse or wallet, there are the persistent offenders who target the same victims on a regular and organised basis.

The Freedom of Information Act, as well as delivering improved transparency regarding how our government offices work and generally serving the greater good, also means that fraudsters can legitimately gather intelligence on their potential targets. For example, Her Majesty's Revenue and Customs (HMRC) will, if asked, release data on the newly retired, lottery winners and the rich.

3 TYPICAL TYPES OF FRAUD

The typical types of fraud directed at elderly people and the retired are ...

- Door to door sales of rotten foodstuffs, inferior products and services.
- Distraction burglaries
- Telemarketing scams
- Postal scams
- Mail order scams
- Financial mismanagement
- Abuse of Enduring Power of Attorney and Guardianship

Door to door sellers

We've all seen them but what about being on the receiving end when this type of caller appears on your doorstep? Not only are they uninvited, very often what they are selling be it a product or a service, is not wanted, needed or worth the money.

Try this ...

Think for a few moments of what it must be like to face such a caller if for example, you are elderly, live alone and are feeling lonely or unwell.

Try to imagine ...

- What thoughts would be going through your mind given that there is a stranger at your door?
- What emotions would you be experiencing as you prepare to answer the caller?

Compare your own answers to the Response Sheet on page 38.

No doubt you will have identified thoughts and feelings similar to the ones listed on the response sheet. You may have personal experience to draw upon such as an elderly parent or relative who has been visited recently by a cold caller. The key thing to realise is that how these callers present themselves not only has a direct bearing on their success at plying their trade, it affects how the householder subsequently feels about the whole experience. To a large extent it determines whether or not they are able to cope with the consequences of this type of approach.

In October 2008 Mr Myatt, a blind pensioner in Birmingham, died after he was targeted by doorstep conmen. They are thought to have posed as community service personnel to gain entry to Mr Myatt's home. In the incident the two men are thought to have pushed Mr Myatt who suffered a kidney injury from which he died. The men escaped with a small amount of change.

A resident answered the door to an official from a local hospice. This person presented what turned out to be an out of date identity badge from the hospice and gained entry by saying he could explain things better if he came inside. Fortunately the elderly resident refused entry and he left eventually. Whilst it may seem rude telling someone to go away that is exactly what needs to be done with unexpected callers who either want to sell you something or say they need to come into your house.

An elderly lady was cold called by a man who asked if she wanted to buy a carpet which he would fit for her. She agreed but said she could not get to the bank. He offered to drive her to the cash machine and she accepted withdrawing over £800. The man carried the carpet to her bedroom and left saying he'd be back shortly with the fitter. No one returned and she later discovered that her bag was missing.

Elderly residents are easy to find as many live in low-rise accommodation often laid out in hamlets of bungalows distinct from other types of accommodation.

Persistent offenders will visit an estate of old peoples' bungalows at least twice a year with the intention of robbing them either as a 'fish seller' or distraction burglar. The fish sellers are people who have rotten or nearly rotten fish that they hawk from door to door and dupe their victims into buying. They hype up the benefits of buying today at their price compared to the price in the local stores and ramble on about how much more convenient it is to buy now and freeze rather than having to go regularly to the shops. What they don't tell their customer is that the stuff is bad and the price is grossly inflated.

Whether they are friendly and appear kind or are brusque, intimidating or even threatening the aim of these cold callers is the same - they are intent on coercing as many people as possible into buying their garbage.

So if it's not fish they are selling the same tactics apply equally to other commodities and services. Pressure is put on people to buy there and then. Make no mistake, these people peddle fear. It may be disguised as doing someone a favour by offering an absolute bargain. On the other hand it may be "buy or else" tactics which they use. The result is the bargain fish is no such thing, the bargain roof repair is a bad joke and the bargain driveway is good for a few weeks if you're lucky.

There is unfortunately a higher price to pay than the actual financial loss although the loss of funds can be significant. What this sort of deception does is rather insidious in that it can alter a person's outlook and perception of others. Some victims try to hide their shame or embarrassment at having been conned by laughing it off or living in denial.

> A member of our family paid an undisclosed amount of cash to a guy who was driving around her estate with a van load of sofas

and chairs. He collared her as she pegged her washing out one afternoon. She believed his story that this furniture was excess stock from some show homes nearby. He told her it was real leather and she believed him even though it most clearly was genuine plastic.

The scary thing is that she let this stranger into her home and that she was alone with him whilst she sorted out her money. Yes cash in the house! To this day she attests to the legitimacy of this transaction and the quality of this furniture even though the rest of the family knows it was a dodgy deal and the furniture is hideous as well as being very uncomfortable!

Others will put this sort of thing down to experience and hope to be more wary next time. Some, however, will feel so bad about the deception that their behaviour changes. They may start to feel afraid and suspicious of everyone who comes to their door or tries to help them when they are out and about. Some will lose confidence and become withdrawn and isolated all of which makes them even more vulnerable. Sadly some will become unwell or suffer a deterioration of an existing health problem from which they may not recover.

Distraction Burglaries and Bogus Callers

'Any crime where a falsehood, trick or distraction is used on an occupant of a dwelling to gain, or try to gain, access to the premises to commit burglary.'

Home Office Rules for Recorded Crime (28.2)

The statistics up to April 2005 read that there were 12,691 reported cases of distraction burglary in England and Wales. Of these 6% involved the use of false pretences to gain entry, however, this increased to 13% among households headed by someone aged 60 or over.

Whilst technically a type of fraud, the police make the distinction and use the term Distraction Burglary to refer to the doorstep crime where an offender seeks access to a person's home with the intent to steal cash and items they can convert to cash.

The elderly and vulnerable in society are for obvious reasons marked as easy targets and given that items of a high sentimental if not monetary value are at risk, the devastation this type of crime causes makes it particularly harrowing for the victim.

To combat this cruel offence Cleveland Police in 2003 launched an initiative they called Operation Strongbow. It had been designed as a purposeful approach to tackling the increasing levels of this type of deception and theft; a level which the police felt was actually much greater than was being reported.

In March 2009 Operation Strongbow was adopted on a regional basis so that the forces of Cleveland, Durham and Northumbria are now working together in a unified and systematic way to make the region a hostile place for those involved in perpetuating doorstep crime.

Similar initiatives are operating throughout the country. Typical key partners working with police forces are Trading Standards, Age Concern, Citizens Advice Bureau (CAB), Local Authorities and Utility Companies to name but a few.

The key features of these schemes are …

- Aside from the overarching aim of ridding the area of such callers and bringing those caught committing offences to justice, all of these schemes share a belief in the effectiveness of education.
- Educating the professionals involved in caring for the elderly and vulnerable, their families, their friends and the person themselves has been shown, through evaluation of some of these initiatives, to reduce the number of incidents.
- Additionally these schemes can show how education has reduced the level of fear amongst elderly residents and thus improved their quality of life.

- Help the Aged provide the Seniorlink Service. This is simply a base unit with a button on it. Whenever a person needs to access the service all they need to do is press the button on the base unit, or the accompanying pendant or wrist strap. The service is operational 24/7 365 days a year. What it does is connect the resident with a Seniorlink response officer who will arrange for help from any of the emergency services. All that is required is a telephone line and a 13 amp socket within 12 feet. In some parts of the country Help the Aged operate a Seniorlink Bogus Caller Scheme.

  This service provides a 'door alert' button adjacent to the front door. When pressed this connects to an operator who can then check the identity and legitimacy of the unexpected doorstep caller. This enables the resident to stay safe behind a locked door. A legitimate caller will not mind waiting whilst the resident checks them out. Bogus callers are more likely to go away to try their luck somewhere else.

What is happening where you live?

Go to www.direct.gov.uk and check out what your local police force is doing to deter and apprehend doorstep criminals. Under the heading "A to Z of Central Government" select the letter 'P' for Police Services in the UK and follow the link to your local force. This link will take you to a map of the UK – just move your cursor to your Region to find the appropriate link www.police.uk/forces.htm.

Find out which agencies are proactively helping the elderly and vulnerable in your area.

Discover what educational services they provide to raise awareness of this type of fraud. What aids and advice do they provide for residents?

Find out what help is available for your elderly relative or friend in the area where they live. Ask your relative if they have been approached by any of the agencies and offered help. Check with them as to what help they accepted.

Chat with them to find out how they feel about this sort of caller. See if there is something else you could do to make them safer and feel safer and more at ease in going about their daily life.

How to reduce doorstep danger. . .

There is a wealth of information in the marketplace. Rather than being a help the volume of information can be a hindrance for it's too time consuming to trawl through. This selection of easily implemented ideas and simple modifications to behaviour represent a straightforward approach to fraud prevention, cutting out the need to search here, there and everywhere.

Any of the following suggestions will contribute to safer living. Many of these suggestions can be carried out by the person themselves. Others will require help which is where family and friends and care professionals come in.

First and foremost perhaps the most important thing to understand is that the habits of a lifetime are unlikely to be broken in a person of advancing years.

Rather than waste valuable energy arguing with people who simply will not accept that buying from doorstep callers is fraught with danger, concentrate your efforts on doing things to reduce exposure to this risk.

The following are aimed at deterring cold callers and therefore protecting the elderly from the harm and distress they can cause.

How to keep relatives and friends safe

You can download these bullet points in the pdf toolkit here. You can then print them off for, or email them to, your relatives and friends.

- Have as good a quality door as you can afford. Avoid those with large areas of single pane glass as this can be easily broken.
- Have mortise locks fitted and use them.
- Do not leave your keys in the door or near to the letterbox where somebody could grab them.
- Get a door sticker. These are being used in Operation Strongbow and carry the message, "I do not speak to uninvited callers". They have the advantage that they allow the person to say no without having to open their door. Even if they do answer the door all they need do is to point to the sign.
- If you choose to answer the door always have the chain on.
- Have a small card to hand which explains that you do not buy from doorstep sellers. If you have difficulty saying "No" the card does it for you.
- It is a good idea to speak through the door to an uninvited caller. Do not engage in conversation other than to give a short, appropriate response such as ...
    - No thank you
    - Sorry I can't help you
    - I don't need it
    - I have people who will do that for me
    - Show me your identification
    - I'll check with your company.
- Register with the Seniorlink Service (see page 18) provided by Help the Aged.
- Never give out personal information such as your name, telephone number, where you bank, whether or not you have money in the house, or disclose that you are alone, are going out or going away soon.
- If the local police force/trading standards is operating No Cold Calling Control Zones similar to the familiar Neighbourhood Watch scheme find out how to become involved. These schemes make it obvious that doorstep callers will not be tolerated without the need for residents to agree to it. This spares them from a potentially upsetting altercation with a stranger and reduces their risk of falling victim to doorstep crime.
- Have a peep hole fitted so that callers can be seen without the door being opened.
- When answering the front door ensure the back door is locked. This is because distraction burglars often work in pairs. Whilst you are distracted

by one persona second person enters by the back door and is rifling through your property.

- Have a two-way intercom fitted. You can then speak to callers without having to open the door. If you live in a block of flats check out who the caller is before you buzz them into the building.
- Social alarms provide immediate access to help if you are in distress, not only from a purely medical standpoint.
- See if there is a family member or close friend who could come round immediately should there be a problem with a doorstep caller. In the event of being pestered, having someone who could come to your assistance can be a comfort to you and a deterrent to the caller. Keep a postcard by the telephone with the numbers of family and friends who can help at short notice or have their numbers on speed dial in your telephone.
- Have a good and functioning external light covering your doorstep and entrance.
- For important documents that need to be kept at home secure them in a lockable metal box or cabinet or some type of lockable cupboard. If possible keep knowledge of this limited to people you trust. The less number of people who know about it the better.
- Report unlit street lights to the Council. Darkness and dimly lit areas make it easier for opportunistic thieves and rogues to lurk.
- If you have a home help be fair to them and keep temptation at bay by ensuring they do not have access to your personal information such as identity details and bank account numbers. That's not saying everyone is a thief and fraudster but we can never know who knows who and what pressure a person may be under to do something unexpected, like steal your identity and pass to criminals who will use your identity to buy goods and services fraudulently. A colleague of mine had their identity stolen a couple of years ago. Someone pretended to be them, purchased a car in their name and paid for it with his PayPal account. Whilst he didn't lose any money the seller of the car lost the car and didn't get any money for it. As if that wasn't enough the fraudster directed the seller to my colleague's website so they could see a picture of him and presumably be convinced they were doing business with a reputable person.
- Register with the Telephone Preference Service. This is a free service that blocks unsolicited telephone calls. This can be important because some doorstep scams involve agents who telephone to arrange for a representative to call in person. They use the telephone call to gather information from you that is then used by the personal caller as part of their patter to get a sale.

- Use the Caller ID facility on your telephone and do not answer calls from numbers you do not recognise.
- When you need a tradesperson check out the government sponsored Trustmark Scheme. It's all about finding an honest trader and steering clear of the rogues.
- Sign up to the Mail Preference Service. It's free and it stops the majority of junk mail that is usually offering freebies that are mere trifles compared to the price of the goods and services they are enticing the public to buy. If it doesn't come through the door in the first place there's no danger of temptation.
- Follow the author Bill Bryson's lead and take pleasure in folding everything so that it fits inside the post paid envelope and send junk mail back where it came from. The sender soon takes your name off their database!

Reduce your exposure to dodgy doorstep callers!

Use this Risk Assessment Grid, on the next page, to check out what dangers you or your relatives are exposed to and the level of harm you could face. Identify which control measures you could adopt to reduce your level of risk. The examples already entered on the grid show how the grid is intended to be used.

You can download this Risk Assessment Grid in the pdf toolkit from here**.** You can then print it for, or email it to, your relatives and friends.

Use the following ...

Legend: Risk rating = Likelihood x Severity

Likelihood	**Severity**
1 = Unlikely	1 = Minor impact
2 = Possible	2 = Major impact
3 = Probable	3 = Critical impact

RISK	LIKELIHOOD	SEVERITY	RATING	CONTROL MEASURE
Losing a few pounds to a doorstep conman.	2= Possible	1 = Minor impact	2 x 1 = 2	Perhaps listen to but do not buy from.
Losing several hundred pounds to a doorstep conman.	2 = Possible	2 = Major impact	2 x 2 = 4	Do not listen to and deter with a door/window sticker.
Losing several thousand pounds to a doorstep conman.	2 = Possible	3 = Critical impact	2 x 3 = 6	Have door/window sticker. Never speak with doorstep sellers. Do not open the door to.

Telemarketing Scams

New technologies pose new risks for older people.

Conducting commercial transactions over the telephone appears to present an easy alternative to the more conventional ways of buying products and services. Times change.

The next generation of elderly people will likely be more familiar with telephone and internet shopping. That's not to say they will necessarily be any the wiser.

Already there seems to be a cloud of complacency hanging over the issue of fraud, with people of all ages shrugging it off as a mere sign of the times, along with a "it's bound to happen" sort of attitude.

Beware the telephone scam …

Telemarketing fraud can be described as the unlawful practice of marketing for the express purpose of inducing a person to buy, donate or invest personal money through a deceptive scheme.

Such schemes are set up to limit the benefit to the customer while maximising the profit to the seller. Similar scams are frequently perpetrated over the internet.

In the United States it has been estimated the $40 billion is lost each year to the fraudulent sales of goods and services over the telephone. (Source is the Australian Institute of Criminology Conference June 2001 – Dr Adam Graycar and Marianne James))

The US survey found …

US survey said	56% of telemarketing fraud victims were aged 50 years or older
US survey said	Most victims were well educated, had above average incomes and were socially active
US survey said	Less than 5% thought a telemarketer could be a criminal
US survey said	40% said that they could not tell the difference between a legal and an illegal telemarketer.

Source Aziz et al 2000 cited in Australian Institute of Criminology presentation to Conference June 2001.

An alarming fact is that repeat victimisation of older people is widespread with lists of victims sold on the black market.

In Kent recently many older residents reported to Trading Standards that they had received hard sell telephone calls from a security company. This company targeted people who already had burglar alarms using scare tactics by suggesting that crime in their area was increasing and so make an appointment for an upgrade.

Some people were told they were entitled to as much as £1500 in free equipment if they make an appointment. It is possible this company would then use sales tactics to get people to buy inferior products they do not need and perhaps sign bogus agreements. Once inside the resident's property they could conceivably wear them down with all sorts of pressures, possibly obtaining bank details and cash payments for goods that may or may not be delivered.

A resident in Herne Bay was telephoned by someone claiming to be an official from the local council. This person told the resident they had overpaid on their council tax and to process the refund needed the resident's date of birth. After being given it the caller rang off. The resident's credit card was later used to buy goods fraudulently on the internet.

So what can you do?

Fraud is a risk we all face and, as is the case with other risks in this life, surely the most sensible thing to do is manage the risk. However knowing what to do and doing what you know are two different things. So we have situations where people go to the "nth" degree to manage risks in the workplace yet give little or no regard to their or their family's domestic exposure to risk in general and fraud in particular.

For example, an associate of mine is responsible at work for his firm's exposure to possible loss through insider fraud of intellectual capital; to the point where he can be a social bore harping on about safeguards and gateways. Yet at home he and his wife pay no mind to the credit cards and personal papers they leave in plain sight for their cleaners and trades people to peruse.

Using the basic principles of risk management and applying them to the home situation of an elderly person, the following are straightforward and effective ways to minimise the likelihood of being defrauded by a criminal telemarketer.

As far as telephone callers go we can ask the caller to verify they are who they say they are by asking for the full company name and telephone number. We can then call the number if it's UK based or otherwise hang up. Do not dial 09 numbers for these are very definitely scammers. We can tell the caller we will check them out and so they can call back later, the rogues will not bother. Don't be afraid to change your behaviour, the legitimate caller won't mind your questions or reservation about discussing business over the telephone.

Steps for safer shopping using a computer and care regarding mail shot promotions

You can download these bullet points in the pdf toolkit here**.** You can then print them off for, or email them to, your relatives and friends.

- Join the Telephone Preference Service (TPS). This is a free service. You can also contact them by telephone - 0845 070 0707.
- If you decide to join the national "do not call" list be aware that this is a monthly subscription service. It is available at http://www.callpreventionregistry.co.uk. You can call 0800 652 7780 for their out of hours 24hr answering service, leave your details and they'll call you back.
- Activate the Caller Identity facility on your telephone by making sure you have the appropriate phone and contact your telecoms service provider.
- Do not answer calls from numbers you do not recognise.
- Do not leave personal papers such as bank statements, bank cards, credit cards and receipts and insurance documents where others can look at them. Home helps, cleaners and trades people should not be put in the position where they are tempted to peruse your personal documents.
    - Although you may well trust them, sometimes peoples' circumstances change resulting in some turning to fraud to help them out of a tight spot.
    - Then there are those who gain trust only to commit a fraud - why? because they can.
    - Too often it's a person known to the victim who either intends a fraud or is instrumental in initiating one.
- Get into the habit of contacting Trading Standards about companies and services that have been offering unsolicited products and service over the telephone or through a mail-shot. Trading Standards will give up-to-date information about the company and offer consumer advice. They work closely with the police and rely on the public to alert them to possible fraudulent trading activity.
- Arrange for a relative or friend to be present at any meeting you have agreed to with a potential service provider.
- Do not pay for services before you have received them.
- Read the privacy terms of any internet sale checking for what they will do with your personal information. If in doubt back away from the transaction.
- Always look for the closed padlock symbol when paying for goods and services on the internet. If it's not there **Do Not Use The Site**.

You will find the padlock on the bottom line of your browser ...

- Have spyware and firewalls installed and activated on your computer. Update them daily. Ask someone to help you if you are unsure how to do this.
- Protect your computer based data with passwords. Do not tell others your password and if you must write them down disguise them in some way so that to anyone reading them it would not be immediately apparent what

they were. Create user passwords that you can remember but that are not obvious to most people such as pet's name, nickname, and birth date.

- Get into the habit of sourcing products and services for yourself rather than responding to the telemarketer, glossy brochure or mail shot promotion.
- Get into the habit of comparing products and services before you make your decision to buy. That may mean going to different outlets to see the quality of the product. It may mean getting prices from different suppliers. It may mean asking for and checking references from satisfied customers. **Doing some work yourself could well prove to be the difference between being satisfied and being scammed!**
- Visit the government information website at www.direct.gov.uk for information on how to stay safe on the internet.
- If children are likely to use the computer restrict internet search through reputable filter search engines only.
- If children use the computer they should be monitored by a responsible adult.
- Never share account details, usernames, PINs or passwords.
- Use a low credit limit card for all your internet purchases
- Print out a copy of your order or transaction.
- Check bank statements for correct payments and report discrepancies to your bank without delay.
- Abort a transaction if you get directed to a different site or multiple sites that do not display security features
- Do not give personal details away on networking websites. Refrain from disclosing personal history and habits such as where you socialise regularly, where you live and work as your data is unsecured on such sites.
- Make a habit of reading the privacy and security policies of the sites you visit that ask you to enter identification details and personal information.
- Never respond to e-mails asking for account details, PINs, passwords or personal information.
- Never respond to e-mails suggesting you are the subject of a Revenue and Customs inquiry or appear to come from a government agency for it is not their policy to communicate such matters by email. Report the message to the appropriate body either by telephone or in writing.
- Similarly do not respond to emails that look kind-of official but also suggest something is not quite right. Instead telephone the official body in question using the contact numbers in the telephone book, from directory enquiries or on official correspondence you have received from them in the past.

- Ensure the spam filter on your computer is always switched to ‘On’. Again ask your family to help
- Update your computer security system(s) on a daily basis to protect against ‘phishing’ - this is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication, ‘pharming’ - this is a hacker's attack aiming to redirect a website's traffic to another, bogus website and virus scams and infections.
- Empty your spam folder regularly taking care not to open any of the messages.

If you suspect that your elderly relative is using a computer for shopping but has very little savvy when it comes to modern technologies, suggest that you'll help them search and buy. That way you are helping them be independent but reducing their exposure to the risk of fraud.

Introduce the subject of fraud when chatting with your elderly relative. Do so in a conversational way rather than try to lecture them. Only by making people aware will they begin to know how they could fall prey to a fraudster and thus want to do whatever they can to prevent it.

By giving people an understanding of this problem it is hoped they will be minded to help themselves wherever possible, and be helped where necessary.

Internet dangers

The use of home computers by older people heightens their exposure to fraud and increases the likelihood that they will at some stage be duped in some way. Indeed it was reported in the press and television as recently as March 2009 that an old gentleman in Scotland had fallen prey to such a fraud resulting in him actually losing his house.

It is interesting to note that the Fraud Act gave responsibility to the banks to accept responsibility for credit card losses. People should call their bank to report the fraud. In the case of significant losses the bank should investigate to a degree then refer the matter to the Police Economic Crime Unit. For a useful site see www.met.police.uk/fraudalert. Given that only 13 such referrals were made to Northumbria police in the twelve months up to 25.3.09 would suggest that the banks are reluctant to admit to the scale of the problem. It's no wonder that people shrug their shoulders when their card is cloned or the goods never materialise from an internet transaction, they just see it as the way of the world nowadays.

Cyber crime is big business and because our personal details are held on many, many servers throughout the world each one of us ought to care more about who we give our information to. We need to adapt our behaviour and refrain from being so trusting.

Where the internet is concerned however, we do not have the advantage of a person to speak to. This means that we can easily be lured in by authentic-looking websites. We are bombarded with product and service claims and images we have no way of authenticating. Follow the precautions listed on pages 26, 27, 28, 29 and 30 to make your internet use and shopping experiences safe.

While older people are not the only ones who are being defrauded through the use of computers, their vulnerability is significant given that it is fair to say that many do not have a full understanding of the technologies they are using.

Property repairs

The minor building works category of home repairs presents a particular problem for older people. Fraudsters and scammers play on fear and pressurise older people into having work done. Often the work is sub-standard and all too often is totally unnecessary.

It is usually roof repairs, chimney repairs and guttering simply because they are difficult for the older person to see and inspect for themselves; hence they take the word of the 'knight in shining armour' who just happens to have noticed as he was passing, or when doing work on a neighbour's property!

This is an area where the older person needs the protection provided by No Cold Calling Zones or at least a door sticker deterring cold callers.

The more difficult thing is the education of older people about the dangers of rogue builders and odd-jobbers. Many old people live independently and as such are free to answer their door to anyone, engage in conversation and be influenced by less than honourable people. By deterring such callers in the first place, vulnerable older people will be better protected without them having to worry about learning how to say 'No'.

Local Trading Standards offices have schemes running aimed specifically at protecting the older resident. They work in partnership with the local authority, police and charities and offer a wealth of consumer safety help and support to older residents and their carers.

Guidance Tips are available both in this Useful Guide and also as a printable file in the toolkit. It provides hints and tips, presented in a user-friendly style, covering the many simple things that can be done to reduce exposure to doorstep, telephone, mail and internet fraud.

Don't forget, when you need a tradesperson check out the government sponsored Trustmark Scheme.

4 Know your rights

Whilst many doorstep sellers are genuine some are most definitely not. It matters that if you do choose to purchase goods and services in this way you know your rights.

The Doorstep Selling Regulations

The Cancellation of Contracts made in a Consumer's Home, or Place of Work etc. Regulations 2008 came into force on 1st October 2008.

They apply where any product or service is supplied costing £35.00 or more.

The Regulations work best if contracts for goods and services are made in writing rather than wholly verbal.

They cover such purchases whether conducted in the person's home, place of work, another person's home, or on an excursion organised by the trader away from their business premises.

The Regulations set a minimum cooling off period of 7 days and require the trader to show cancellation rights clearly and prominently at the time of the sale.

The notice of cancellation rights must be dated and given to the customer at the point of sale. Failure to do so is a criminal offence.

Where you agree to have work started during the 7 day cooling off period and then decide to cancel, you will be required to pay for the work done so far.

If you have not agreed to receive services or goods during the cooling off period but the trader starts work or makes a delivery, you are not obliged to pay.

To cancel a contract you must ...

- Cancel in writing and post (or hand deliver), or email the trader.
- Do this within 7 days of signing the contract.
- Keep proof of cancellation.

Remember that cancellation is effective on the day you post, deliver or email your notice NOT the day the trader receives it.

You must return any goods to the trader that you are not required to pay for.

You will need to pay the postage for any returns

You are not required to return the goods until you have received your money back.

As soon as the contract has been cancelled it will be treated as never made meaning that the trader should return any money that you have paid, including any deposit.

These Regulations do not apply to contracts with a value less than £35.00.

Nor do the Regulations apply to contracts for food and drink delivered by regular roundsmen and insurance contracts.

Before you make any doorstep purchase, ask yourself ...

You can download these bullet points in the pdf toolkit here. You can then print them off for, or email them to, your relatives and friends.

1. Does this doorstep seller provide anything in writing?
2. Can they provide some valid form of identification?
3. Can they show that they have business premises elsewhere?
4. Do they have a business name?
5. Have I ever heard of them?
6. Do I have to respond here and now, what's the rush?
7. Does what they are flogging look too good to be true?
8. Do I have to give my bank or credit card details?
9. Do I have to part with a significant amount of cash?
10. Can I afford to lose the money?

As a guide if you answer questions 6, 7, 8 and possibly 9 with a 'Yes' walk away for you are in grave danger of being scammed.

If your answer to question 10 is 'No' that's exactly what you should say to the caller, and keep saying until they go away!

5 Useful websites and telephone numbers

Reporting Fraud

National Fraud Strategic Authority – www.attorneygeneral.gov.uk

020 7271 2460

Home Office – www.homeoffice.gov.uk

Area Police Economic Crime Units – www.met.police.uk/fraudalert/

Consumer Issues

Trading Standards Institute - http://www.tradingstandards.gov.uk/

08454 04 05 06

Telephone Preference Service – www.tpsonline.co.uk

0845 070 0707

Mail Preference Service – www.mpsonline.org.uk/mpsr/

0845 703 4599

Call Prevention Registry – www.callpreventionregistry.co.uk

0800 652 7780

Consumer Direct - www.consumerdirect.gov.uk

08454 04 05 06

Trustmark Scheme – www.trustmark.org.uk

01344 630 804

Advice and Guidance

Directgov - www.directgov.co.uk

Caring dot com - www.caring.com

Direct Marketing Association – www.dma.org.uk

020 7291 3300

BT Privacy Service - 0800 916 5544 (free)

Seniorlink Service – www.seniorlink.com/

Seniorlink Bogus Caller Scheme –

www.helptheaged.org.uk/en-gb/AdviceSupport/HomeSafety/BogusCallers/

Response Sheet

Possible thoughts could include ...

- I wonder who this is?
- Who could be calling at this time?
- I wasn't expecting anyone…
- Oh dear, who could this be and what do they want?
- What a nuisance, I was just going to have something to eat.
- I'll give this person what for, pestering me at this time.
- Oh good someone to chat to
- Oh good, someone to have a bit of fun with for I don't want to buy anything really.

Possible feelings could include ...

- Anxiety
- Nervousness
- Excitement
- Frustration
- Annoyance
- Fear
- Irritation
- Anticipation
- Curiosity
- Tension
- Relief
- Embarrassment

7 Some additional reading

The Madoff story

Described by the financial services world as a fraud of spectacular dimension the financier Bernard Madoff allegedly cheated his hedge fund and investment banking business of at least $50billion.

Interestingly he was highly regarded and his hedge fund appeared very successful, attracting investors keen to get a slice of the action. Hedge funds work by allowing investors to deposit a set amount for a set period. A good fund such as Madoff's was believed to be will make money even in a depressed market. The lure of splendid returns along with the presumed safety of a good and well managed fund attracted the very institutions we bank and invest with; such is today's global marketplace.

Bernard Madoff created a false sense of security and generated the belief that his hedge fund was successful. He did this by using money from new investors to pay other investors promised returns of up to 12%, thus giving the impression the fund was profitable. In turn this encouraged new investors who in all probability felt secure given Madoff's reputation as a successful businessman.

The reality was the fund had not been successful for quite some time but whilst ever the wholesale financial market was buoyant and investors were getting their money, the truth could be hidden. It was when markets dried up resulting in no new investors it came to light that Madoff could not pay his old investors. As a consequence the fraud was discovered.

The name given to this type of fraud is pyramid or ponzi scheme where money from new investors is essential because this is where the money comes from to pay old investors.

The real shock in this case is that it went undetected for so long and remained hidden from the United States authorities (the Securities and Exchange Commission) through not one but two separate investigations, one in 2005 the other 2007. Madoff admitted that he began the fraud in the 1990s as he tried to navigate the depression at that time, intending to extricate himself from the scheme when the markets picked up. Whether unintentionally or by design he never did and so just got deeper and deeper into it. He alleges that he acted alone and in June 2009 was sentenced to 150 years in jail for what turned out to be a staggering fraud of $65b (£38b) and a massive breach of trust.

This was an extensive fraud both in the United States and abroad and with UK banks and financial institutions having "bet" on Madoff's fraudulent scheme losses may be closer to home than some of us care to think.

The Darwin story

The Darwins presented themselves as an ordinary but slightly better off than most sort of couple. John Darwin had worked as a school teacher and prison officer his wife Anne worked as a receptionist. Despite having a portfolio of properties available for rent mainly in County Durham the couple who lived in Seaton Carew on Teesside, couldn't make ends meet.

Rather than sell any of the houses they chose instead to embark on a scam that would see them amassing a fortune of up to £500,000 and a very comfortable lifestyle in Panama City.

In 2002 John Darwin faked his own death and his wife actively assisted. He went out in a canoe and some time later his wife reported him missing. In fact she had driven him to Durham railway station from where he travelled and hid in the Lake District for several weeks. In spite of the best efforts of the emergency services no trace of Mr Darwin was found. Mrs Darwin apparently put on a good show even though after a few weeks she was in fact living back with her husband at their Seaton Carew home. When visitors called he hid in an adjacent bedsit that they owned. Relatives including their two adult sons and friends believed him to be dead.

After Mr Darwin was officially declared dead his 'widow' collected some £250,000 in life insurance and pension payments. The pair added to their fortune when the property boom came and Mrs Darwin sold some of the rental properties. It was Mrs Darwin's jet-setting lifestyle and talk of foreign investments which led to a covert financial inquiry by the police, based on an anonymous tipoff. The inquiry became an open one when one evening in December 2007 John Darwin walked into a London police station, saying he had last his memory.

The subsequent inquiry and prosecution revealed the extent of their financial gain as well as the true cost of all the lies and deceit, betrayal of their two sons. The police stated after the trial that this couple worked together in planning and executing this scam. They intended to defraud the insurance companies and pension providers for their own financial gain. Arguably the bigger fallout is the cost to the lives of their sons for neither had anything to do with this scam. What must they think of their parents now and feel towards them and do fraudsters care?

John Darwin is serving a prison sentence of 6 years and 3 months. Anne Darwin was sentenced to 6 years and 6 months. The police and authorities are engaged in asset recovery.

About the Author

Janet Hope, the author of A Useful Guide to Fraud Prevention, is an experienced Training and Development Consultant. Her qualifications include...

- MSc in Leadership & Organisational Change.
- Certificate in Management Studies.
- Certificate in Education.
- CIPD Level IV Training and Development.
- Fully Accredited coach - The Coaching Academy.
- Certificate in Counselling.

Janet Hope is a former fraud investigator and fraud manager for central and local government. Janet used her MSc dissertation to investigate fraud within the small business sector. This Useful Guide to Fraud Prevention is her latest contribution to the focus on fraud. It is presented in the hope that it provides a fresh and practical approach on how to protect oneself and one's family

As we are always trying to improve our Useful Guides we would appreciate any feedback you can give us on **A Useful Guide to Fraud Prevention.** Please click on the link below to access our online feedback form …

http://www.pansophix.com/useful-guide-feedback.html

If we use your feedback to improve **A Useful Guide to Fraud Prevention** we will email you a copy of the updated version.

You can register to access our free online Learning Support Centre which contains a growing range of mental exercises, tips and tools at …

http://www.pansophix.com/learning-support-centre/index.php