THE LITTLE BOOK OF BIG SCAMS

THIRD EDITION

METROPOLITAN POLICE

TOTAL POLICING

One of the mysteries of the con-man is why he bothers. (I say he, but of course there are plenty of con-women who are just as unscrupulous). He is often energetic, imaginative and ambitious, so why doesn't he build up a decent, respectable business instead of robbing hard working people? I suppose it's because con-men (and I've met many over my years in consumer protection) all regard the people they deceive simply as walking wallets, to be ruthlessly squeezed, emptied, and then thrown away. And since we launched the new helpline for older people, The Silver Line (0800 4 70 80 90) I have become aware that some of the most unscrupulous criminals target older people precisely because the older generation, honest themselves, trust other people to be as honest as they are.

So the conmen will shamelessly lie to us, try to tempt us with "something for nothing", "too good to be true" offers – like the "show house" discount for double glazing or central heating, or the "million pound lottery" he pretends you have won and so on.

BIG SCAMS

And he gambles on the fact that when we discover that we've fallen for his blatant swindle, we will be too ashamed to report him to the police or the Trading Standards officers.

I bring you good news. In this excellent booklet, the police are arming us with the best of all weapons to defend ourselves, that is, good information and a timely warning. I urge you to read this booklet, even if you think you could never fall for the con-men's tricks. Bright people, honest people, find it difficult to believe that swindles can arrive through your letterbox, in your inbox, on your doorstep. But they can, alas, and they do, and scams like the one described in this booklet deceive good people into losing millions of pounds every year.

So congratulations to the dedicated police team who have created this booklet because they are determined to protect us, and prevent the con-men succeeding. And enjoy this booklet, it's an excellent read and it could save you a great deal of money you can't afford to lose.

Esther Rantzen

CONTENTS

BIG SCAMS

INTRODUCTION

We are pleased to bring you the third edition of 'The Little Book of Big Scams'. We were originally inspired to create the book by a publication created by the Australian Competition and Consumer Commission.

The second edition was very well received and we have distributed over 110,000 copies to London residents, community partners and other agencies. Links to the digital copy of the book have also been adopted on numerous websites.

Since the second edition was published there has been significant change in the way the Metropolitan Police investigate fraud allegations. The Met now has a dedicated team of over 200 officers involved in the investigation of fraud under the banner of FALCON – Fraud and Linked Crime Online. The creation of this unit has seen a significant rise in arrests in London relating to fraud allegations.

In this third edition of 'The Little Book of Big Scams' we have added some new scams that have come to notice, for example concerning holiday accommodation and event tickets and have updated our information and advice on the other scams detailed in the book.

The book should be seen as a general guide to many of the scams currently operating in the UK and we hope it will increase your awareness of these scams and teach you some easy steps that you can take to protect yourself and others.

Every year the British public loses billions of pounds to fraudsters who bombard us with online, mail, door-to-door and telephone scams.

Scams, or frauds, can be difficult to investigate. They can be complicated and often involve many victims and suspects and enquiries outside of the UK. They can take a lot of resources to investigate and courts may find it difficult to convict suspects because of the grey area that may appear to exist between dishonesty and sharp practice.

Prevention, through awareness, is therefore a vital tool in combating scammers.

Scams do not discriminate

Scams target people of all ages, backgrounds and income levels. The Metropolitan Police FALCON team has seen the devastating effects this type of crime can have on people and their families. One of the best ways to fight the scammers is to take steps to prevent yourself from being caught out in the first place.

Some adults may be especially vulnerable to financial abuse. Consider liaising with your local Social Services safeguarding adults department if you are concerned about someone you know who may be vulnerable. When contacting your local Social Services ask for Adult Social Care.

FALCON
FRAUD AND LINKED CRIME ONLINE

Protect Yourself

If you want to stay on top of scams, visit the Metropolitan Police Fraud Alert website at www.met.police.uk/fraudalert which contains current information on the different scams targeting consumers. It also provides tips on guarding yourself against scams, new scam stories, scam alerts and advice on reporting scams.

10 GOLDEN RULES

Remember these 10 golden rules to help you beat the scammers.

1. **Be suspicious of all 'Too good to be true' offers and deals. There are no guaranteed get-rich-quick schemes.**
2. **Do not agree to offers or deals immediately. Insist on time to obtain independent/legal advice before making a decision.**
3. **Do not hand over money or sign anything until you have checked the credentials of the company or individual.**
4. **Never send money to anyone you do not know or trust, whether in the UK or abroad, or use methods of payment that you are not comfortable with.**
5. **Never give banking or personal details to anyone you do not know or trust. This information is valuable so make sure you protect it.**
6. **Always log on to a website directly rather than clicking on links provided in an email.**
7. **Do not rely solely on glowing testimonials: find solid independent evidence of a company's success.**
8. **Always get independent/legal advice if an offer involves money, time or commitment.**
9. **If you spot a scam or have been scammed, report it and get help. Contact ActionFraud on 0300 123 2040 or online at www.actionfraud.police.uk Contact the Police if the suspect is known or still in the area.**
10. **Do not be embarrassed to report a scam. Because the scammers are cunning and clever there is no shame in being deceived. By reporting you will make it more difficult for them to deceive others.**

IMPORTANT INFORMATION FOR ALL UK BANK CUSTOMERS

Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers and other officials or companies in a position of trust. Often the fraudster will claim there has been fraud on your account and that you need to take action.

Your bank or the police will never:

- Phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name.
- Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.
- Ask you to purchase goods using your card and then hand them over for safe-keeping.

If you are given any of these instructions, it is a fraudulent approach. Hang up, **wait five minutes to clear the line**, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud.

If you don't have another telephone to use, call someone you know first to make sure the telephone line is free.

Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller.

Financial Fraud Action UK

www.financialfraudaction.org.uk

BIG SCAMS

IDENTITY FRAUD

Identity fraud is often quoted as 'Britain's fastest growing crime.' It involves the misuse of an individual's personal details in order to commit crime. These personal details are very valuable and they can be misused or sold on to others.

Victims of identity fraud often report a great deal of stress and cost in trying to clear matters up after the fraudulent use of their personal information. Many never establish exactly how their details were obtained.

Protecting your Address:

- ⚠ If you start to receive post for someone you don't know, find out why.
- ⚠ Register to vote at your current address (Lenders use the electoral roll to check who is registered as living at a particular address).
- ⚠ When registering to vote, tick the box to opt out of the 'Edited' register to prevent unsolicited marketing mail. (This does not affect credit checks).
- ⚠ Sign up with the Mail Preference Service to prevent marketing letters. (Details on how to do this are at the back of the booklet).
- ⚠ Protect mail left in communal areas of residential properties.
- ⚠ Re-direct your mail when moving home.

Protecting your Bank Accounts:

- ⚠ Be extremely wary of unsolicited phone calls, letters or emails from your bank, or other financial institution, asking you to confirm your personal details, passwords and security numbers.
- ⚠ Regularly check your accounts and chase up any statements and that are not delivered when expected.
- ⚠ Dispose of anything containing your personal or banking details by using a cross cut shredder or tearing up into small pieces.
- ⚠ Always sign up to American Express SafeKey, MasterCard SecureCode or Verified by Visa when you receive your cards, even if you do not intend to use your cards online. This helps to protect you if your card or details are lost or stolen.
- ⚠ If you think someone is misusing your bank account details then report it to your bank.

Protecting your Phone:

⚠ Never reply to unsolicited texts, e.g. texts referring to accident claims, even to try and get them stopped. Simply delete them.

⚠ Sign up to the Telephone Preference Service to prevent marketing phone calls. Details on how to do this are at the back of the booklet.

⚠ If using a 'smart' phone install anti-virus software on it.

Protecting your Computer:

⚠ Keep your computer security programs, such as antivirus and firewall, up to date. Also make sure your web browser and operating system are the latest version. If unsure how to do this contact a computer specialist.

⚠ Be wary of opening links on unsolicited emails you receive. They may contain viruses or other programs that may harm your computer.

⚠ Know how to verify secure web sites if making financial transactions. You can do this by looking at the address line. Normally it will start with http but when you log into a secure site this will change to https. for example; *http://www.mybank.com* is the address of mybank, but if you want to go to the transactions page you log in and the address bar will change to something like *https://mybank/login.com* The address bar may also change colour. A padlock will also appear in either the bottom left or bottom right corner of your browser bar, not on the website.

⚠ If you have received an email claiming to be from your bank, asking that you contact them, think about whether or not it is genuine. If you are unsure do not click on any links in the email. Open another window in your browser and visit your bank's website using your normal method.

⚠ Check the online banking security options your bank provides, some offer free anti-virus and browser security software.

YOUR PERSONAL INFORMATION IS VALUABLE:
TAKE ACTION TO PROTECT IT.

BIG
SCAMS

COURIER FRAUD

Courier frauds are becoming more prevalent and sophisticated. Usually the elderly are targeted. Scammers will telephone a potential victim purporting to be from their bank, from the police or other law enforcement authority. They then dupe the person into revealing their PIN and handing over their debit or credit card.

What you should know

- A scammer rings you, claiming to be from your Bank or the Police, saying a fraudulent payment has been spotted on your card and this needs resolving, or that someone has been arrested using your details and cards.
- You may be asked to ring back using the phone number on the back of your card. This further convinces you that the call is genuine. However, the scammer keeps the line open at their end so, when you make the call, you are unknowingly connected straight back to them or their friends.
- They will ask you for your PIN number or sometimes ask you to key it into your phone's handset. YOU SHOULD NEVER GIVE YOUR PIN TO ANYONE IN ANY WAY.
- The scammer then sends a courier or taxi to pick up your card from your home. It is possible the driver does not know they are being used as part of the scam.
- Once they have your card and PIN the scammer can then spend your money.
- There are now many variations to this scam. One of these is where you are contacted and told there is a corrupt member of staff within your bank, a Post Office or bureau de change and the police need your help to identify them.
- You may be asked to withdraw a large sum of your money with the purpose of the money being marked by the police or bank to be placed back into the banking system. They say this will help them identify the corrupt person. On handing the cash over it is taken by the scammers.

- ⚠ Another variation is being asked to purchase an expensive watch, or other high value item, to try and identify counterfeit goods. You will then be told to hand this item to a taxi driver for transfer to the police. The item is then passed to the scammer.
- ⚠ The latest variation is where you are informed your bank account has been taken over and you need to transfer all the funds in to a 'safe account' set up by the caller. This account is operated by the scammers who then steal the funds.

BIG SCAMS

REMEMBER	Your bank or the police will NEVER ask for your PIN, your bank card or to withdraw money.
CAUTION	NEVER share your PIN with anyone – the only times you should use your PIN is at a cash machine or when you use a shop's Chip and PIN machine.
THINK	NEVER hand your bank card or any goods you have purchased as a result of a phone call to anyone who comes to your front door.
INVESTIGATE	If you think you have been the victim of this scam, call police.

BIG SCAMS

HOLIDAY FRAUD

Holiday frauds are on the increase and holidaymakers are being scammed out of millions of pounds a year by fraudsters. Scammers are targeting online holiday booking and accommodation sites to scam unsuspecting customers into paying for accommodation that is not available or does not even exist. Often the victim only becomes aware they have been scammed when they arrive at their accommodation or destination and find no booking has been made.

What you should know

- ⚠ Scammers will often ask for payment by direct bank transfer away from the website. They may encourage you to do this by offering discounts for bank transfer payments.
- ⚠ Often scammers will use photos of accommodation taken from other sites on the web. You can check photos with a reverse image search engine available on the internet. These check images to see where else on the internet they may have been used.
- ⚠ The scammer's advert may state that they belong to a trade body or consumer protection scheme such as the Association of British travel Agents (ABTA). Contact the body or scheme to check their credentials. Contact details are available at the back of this book.
- ⚠ Try and research the property and see if it has its own website. Always try and call the owner of a property to confirm they are aware of your potential booking. If their phone number is not provided send an email requesting it.

HOLIDAY FRAUD

HOLIDAY FRAUD

BIG SCAMS

REMEMBER	If it sounds too good to be true, it probably is! If it doesn't feel right ask questions.
CAUTION	Check the web address is legitimate and has not been altered by a slight change such as co.uk to org.
THINK	Why am I being asked to pay by direct bank transfer? Use your credit card to pay so that your purchase is protected.
INVESTIGATE	Do your research. Are there any reviews about the company?

BIG SCAMS

MASS MARKET FRAUD – SCAM MAIL

Many people in the UK and overseas are lured by the thrill of a surprise win and find themselves parting with large amounts of money in order to claim fake prizes. Often victims of this particular scam are the elderly and vulnerable. There is a huge range and variety of mass market mail, some of which will be obviously fraudulent and others that will not. Whatever the case you should always be wary of what you reply to.

What you should know

⚠ You cannot win money or a prize in a lottery if you have not entered it. You cannot be chosen at random if you do not have an entry.

⚠ Many Mass Market scams will trick you into parting with money or providing your banking or personal details in the belief that you will win a cash prize. You do not have to pay a fee to claim a legitimate prize (*see Think Jessica page 46*).

⚠ It can only take a single response to a scammer to be inundated with further scam mail. Your name and address will be included on what's known as a 'Sucker's List' and you may receive large amounts of scam mail on a daily basis.

⚠ A fake prize scam will tell you that you have won a prize or competition. You may receive confirmation of this by post, email or text message. There will often be costs involved in claiming the prize and even if you receive a prize it may not be what was promised to you.

⚠ Psychic and clairvoyant scams can also be used to set you up to fall for a lottery scam. If a psychic gives you a list of lucky lottery numbers, don't be surprised if you receive a letter soon afterwards telling you that you've just won a lottery you've never heard of and do not remember entering.
THIS IS ALL PART OF THE SCAM.

MASS MARKET FRAUD - SCAM MAIL

- ⚠ Be aware that items advertised in the post you receive may be marketed as 'High Quality Exclusive Goods' but in reality can be extremely poor value for money. Another marketing technique is to offer a share of a cash prize but to win you must place an order for goods that in fact are not value for money.
- ⚠ Be wary when sending money too, or receiving money from, someone you do not know and trust. This may be a ploy by a scammer to get you to pass money through your bank account that could be stolen from someone else's account.

Technically you may be money laundering and become what is known as a 'Money Mule'. If convicted of money laundering you could be sent to prison and having a criminal conviction can make it difficult for you to obtain financial products in the future and may affect your job prospects.

MASS MARKET FRAUD - SCAM MAIL

BIG SCAMS

REMEMBER	Genuine lotteries will not ask you to pay a fee to collect your winnings.
CAUTION	Never send money abroad or to someone you don't know and trust.
THINK	Don't provide banking or personal details to someone you don't know and trust.
INVESTIGATE	Examine all of the terms and conditions of any offer very carefully.

BIG SCAMS

INVESTMENT SCAMS

The Investment market is extremely vulnerable to abuse by fraudsters. Many emerging markets remain unregulated making it very difficult for authorities to enforce good working practices. Common investment scams include buying rare metals, diamonds or other gemstones, wine, land, carbon credits and alternative energy. Many people have lost their entire life savings to investment scammers. Don't let it be you!

What you should know

⚠ Scammers will cold-call you by telephone and try to sell you investments in emerging markets that they claim will lead to financial gains above the rates of established investments like ISAs. In reality the item offered may not exist or is worthless. Be wary of any investment company cold-calling you – they may be fraudsters!

⚠ Often the scammers will give you details that you might think only a genuine investment company will have. They may have details of previous investments you have made, shares you hold and know your personal circumstances. Be aware the scammers will do their homework and make it their business to know as much about you as possible.

⚠ The scammers will often call you a number of times in an attempt to form a friendly relationship. If you respond in any way they will persist, try and build trust and may eventually persuade you to part with your money. Having obtained some money from you they will probably call again and try to persuade you to "invest" more money, perhaps in a different commodity.

⚠ Scammers may say they are from a reputable investment company, some will say they are stockbrokers or consultants. Always seek independent financial advice before you commit to any investment including checking with the Financial Conduct Authority (FCA) to see if they are a registered company – do not rely solely on Companies House Data.

⚠ Be wary of companies trying to recover money from lost investments on your behalf for a 'one off' fee – this could be a recovery room fraud trying to scam you again! Similar to the initial investment they are likely to know all about your previous investment history.

Pension fraud

⚠ If you are over 55, from April 2015 changes in the law allow you to access your pension savings. You will have control of your pension pot and it is for you to decide how to invest the money.

⚠ Scammers may target you to try and steal your pension savings by persuading you to cash out your pension and put your money into fraudulent and unregulated investments with the promise of high returns.

⚠ If you are under age 55 you can transfer your pension to another scheme. However you cannot access the funds unless you are seriously ill. If you are offered a cash incentive to transfer your pension be aware that you are likely to face tax charges in excess of half your pension savings.

⚠ If you are cold called, receive a text message, email or similar unsolicited approach offering a pension review beware. It may not be someone acting in your best interests.

⚠ Never make a decision based on phone calls, glossy brochures and pushy salespersons. How often do you buy from a doorstep salesperson? So why would you trust someone you have never met, contacting you from a company you have never heard of, with your life savings?

⚠ Always seek independent advice from someone who is not associated with the "sales pitch". If possible research the company. A genuine financial advisor should be registered with The Financial Conduct Authority.

⚠ The golden rule. If you receive a cold call, email, text etc regarding your pension, put the phone down and/or delete the message immediately.

Find out how to protect yourself at www.pension-scams.com

BIG SCAMS

REMEMBER	Do not respond to callers trying to sell you investments. Simply hang up the telephone. Legitimate investment companies will never cold call.
CAUTION	Don't let the company pressure you into buying because they say the offer won't be there tomorrow. Hang up and take a day or two to consider your options.
THINK	Exercise considerable caution when investing your money.
INVESTIGATE	Make sure you know exactly who you are dealing with and always seek independent/ legal advice before committing to any investment.

BIG SCAMS

DOOR-TO-DOOR SCAMS

Many legitimate businesses sell products door-to-door (windows, solar panels, cleaning products, home maintenance, tree surgeons etc.). Gas, electricity and water companies will also visit to read meters. In addition charities may visit to ask for donations or post collection bags for you to fill and leave out for collection.

However, scammers also do the above to part you from your money, gain entry to your home to steal, or profit by posing as charities in order to collect donations.

What you should know

- ⚠ Door-to-door scams involve selling goods or services that are not delivered or are very poor quality. You won't get value for money and you may get billed for work you didn't want or didn't agree to.
- ⚠ Some scammers conduct surveys so they can obtain your personal details or disguise their real intent to sell you goods or services you don't want or need (e.g. unnecessary roofing work or patio replacement).
- ⚠ Door-to-door sales are normally uninvited and the people selling MUST leave if you ask them to.
- ⚠ Even when a genuine business and product is being sold, unscrupulous employees can sometimes still act illegally.
- ⚠ If someone knocks at your front door claiming to be from a company always check their ID. If you are not happy then do not let them into your home.
- ⚠ Never ring the telephone number on the ID card. Tell them to wait outside, shut the door, and ring the genuine number from the telephone book or website.

BE SUSPICIOUS

DOOR-TO-DOOR SCAMS

DOOR-TO-DOOR SCAMS

BIG SCAMS

REMEMBER	If someone knocks at your door, always examine and check their identification.
CAUTION	Never let anyone in your house unless they are someone you know and trust.
THINK	Don't immediately agree to any offer involving a significant amount of money, time or commitment. Seek independent/legal advice first.
INVESTIGATE	If you are interested in what a door-to-door salesperson has to offer, take time to find out about their business and their offer. Shop around to make sure you are getting a good deal. Confirm with charities that they are collecting in your area.

BIG SCAMS

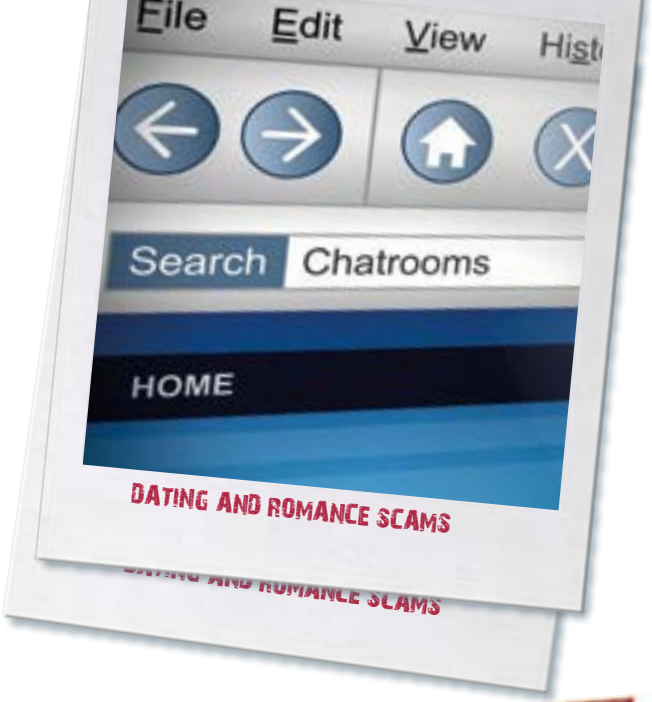
DATING AND ROMANCE SCAMS

Many dating websites and chat rooms operate legitimately in the UK. However, individuals using them may try to scam you. Dating and romance scammers lower your defences by building an online relationship with you. Many people, both men and women, have lost huge amounts of money to online dating scammers. Always consider your personal safety if you arrange to meet someone through a dating website.

What you should know

- ⚠ Be wary of giving out personal information on a website or chat room.
- ⚠ Scammers will quickly interact with you, often showing you glamorous photos of themselves and gaining your trust. But how do you know it is actually the person you are communicating online with? Answer: You don't!
- ⚠ Scammers will make conversation more personal to draw information from you, but will never really tell you much about themselves that can be checked or verified.
- ⚠ Scammers will normally try to steer you away from communicating on a legitimate dating website that could be monitored by staff. Their preference is to communicate via email, text and possibly phone, rather than through the dating website or chat room where you met.
- ⚠ A scammer will use a variety of scenarios to target your emotions and get you to part with your money (e.g. they have an ill relative or they are stranded in a country they don't want to be in and need money). THESE ARE SCAMS.
- ⚠ Never send money abroad to a person you have never met or to anyone you don't actually know and trust.
- ⚠ Scammers will sometimes tell you to keep your online relationship a secret. Never agree to this. This is a ploy to get you not to tell your family and friends who will see the scam for exactly what it is.

⚠ The scammer may ask you to accept money from them into your own bank account. They will come up with a convincing story as to why they can't use their own bank account i.e. discharge fee from their current job, medical care or to pay for essential goods. The circumstances may appear to be genuine; but, you may be committing a criminal offence of money laundering.



BIG SCAMS

REMEMBER	Check website email addresses carefully. Scammers can use illegitimate sites with similar addresses to legitimate ones.
CAUTION	Never send money, give personal information or bank details to a person you have never met.
THINK	Always consider your personal safety if you arrange to meet someone through a dating website.
INVESTIGATE	How can you confirm the identity of the person you are chatting to online? Don't be afraid to ask questions and carry out checks.

BIG SCAMS

BANKING AND PAYMENT CARD SCAMS

Protecting your card details is vital.

Card scams involve the use of stolen or counterfeit cards to make direct purchases or cash withdrawals or the use of stolen card details to buy items over the phone or via the Internet.

What you should know

Phone

⚠ Your bank and the police will NEVER ring you and tell you to verify your PIN, withdraw your cash, purchase high value goods or that they are coming to your home to collect these items, so never hand it over to anyone who comes to collect it. Should you receive a call like this put the phone down. THIS IS A SCAM!

⚠ If you receive a call from your bank or the police, verify who the person is before handing over any personal details. You can do this by calling your bank (the number on the back of your card) or the police (101) on a DIFFERENT phone line. This can be a mobile phone or a phone owned by your family, friend's or a neighbour. If no other phone is available, wait AT LEAST 5 minutes to ensure your line is clear to make the phone call. This is because currently, scammers are able to keep phone lines open. Whilst you think you are making a new phone call, the line is still open to the scammer who pretends to be a different person from your bank or the police (*see page 7 for Courier fraud*).

⚠ Depending on who you bank with, the security questions asked by the bank may vary (e.g. the last 4 digits of your account number or digits of your password) but your bank will NEVER ask you to authorise anything by entering your PIN into the telephone.

ATM – Cash Machines

⚠ NEVER share your PIN with anyone.

⚠ If there is anything unusual about the cash machine or there are signs of tampering, do not use it and report it to the bank as soon as possible.

⚠ Cover your PIN. Stand close to the machine and always use your free hand and body to shield the keypad as you enter your PIN to prevent any prying eyes or hidden cameras seeing your PIN.

⚠ Do not get distracted. Be particularly cautious if 'well-meaning' strangers try to distract you or offer to help you and most importantly, discreetly put your money and card away before leaving the cash machine.

⚠ Fraudsters sometimes fit devices to cash machines that trap your card, which they then retrieve as soon as you have left the area. If your card is retained by the machine for any reason, report it to your card company immediately, ideally using your mobile phone while you are still in front of the machine. Make sure you have your card company's 24 hour contact number stored in your mobile phone.

⚠ If you spot anything unusual about the cash machine, or there are signs of tampering, do not use it. Report it to the bank concerned immediately.

⚠ Once you have completed a transaction put your money and card away before leaving the cash machine. Destroy or preferably shred your cash machine receipts, mini-statements or balance enquiries when you dispose of them.

Banking

- ⚠ Check your statements regularly, including low value transactions. Notify your card company immediately if you suspect a fraud. Dispose of statements or slips which contain your card details carefully and securely by shredding or tearing your documents. This includes your cash machine receipts, mini statements or balance enquiries.
- ⚠ If you have to destroy your bank card then make sure you cut through the card including the CHIP. You can also use a shredder to destroy them.

BIG SCAMS

REMEMBER	NEVER share your PIN with anyone.
CAUTION	Your bank or the police will NEVER ask to collect your card and your PIN.
THINK	Check statements regularly to ensure they are correct.
INVESTIGATE	If you suspect a fraud, contact your bank or the police immediately.

BIG SCAMS

MOBILE PHONE SCAMS

Mobile phones have developed rapidly over the last few years and most now offer a huge range of functions. Smartphones are mini-computers so take all the precautions you would with your own computer at home.

What you should know

- If you use an app to access your online banking, only use the official app provided by your bank. If in doubt, contact your bank to check.
- Only download apps from official app stores, such as Apple iTunes, Android Marketplace, Google, Play Store and BlackBerry App World. Free apps are great but downloading them from unofficial or unknown sources could lead to your device becoming infected with a virus.
- Keep your smartphone's operating system updated with the latest security patches and upgrades. These will normally be sent to you from your operating system provider.
- Do not give your mobile banking security details, including your passcode, to anyone else and don't store these on your device. For added security you should set up a password or PIN to lock your mobile phone or tablet device.
- Just like on your computer, there are anti-virus tools available for your mobile device. Consider using a reputable brand of software. Some banks offer customers free anti-virus software for their mobile phones, so check your bank's website for more information.
- Be wary of clicking on links contained in a text message or email. Don't respond to unsolicited messages or voicemails on your phone. Your bank will never email you or send you a text message that asks you to disclose your PIN or full password.

Types of scam

- Text scams offering you money for an accident you may have had is often a ploy to obtain your personal details. Do not reply – even to 'STOP' texts.
- You may receive a text message or advert encouraging you to enter a competition for a great prize.

The scammers make money by charging extremely high rates for the messages sent from you to them. These could be as high as £2 per text message. Do not reply.

⚠ With trivia scams, the first few questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions you need to answer in order to claim your 'prize' could be very difficult or even impossible. Do not enter.

⚠ If you try to claim your prize, you may have to call a premium rate number (that begins with 0906 for example). You may then have to listen to a long recorded message and there's unlikely to be a prize at the end of it. Do not phone back to claim.

⚠ 'SMiShing' occurs when a scammer sends you a text message asking you to provide personal and/or financial information. The message may appear to be from a legitimate company, like a mobile phone provider. Legitimate companies will not ask you to provide sensitive information by text. NEVER reply to these types of text messages

⚠ Unless you are using a secure web page, do not send or receive private information when using public Wi-Fi.

⚠ Be aware of who is around you when using a mobile device to go online.

BIG SCAMS

REMEMBER	Install antivirus software for your Smartphone if you use it like a computer.
CAUTION	Do not reply to unsolicited text messages.
THINK	Is this a product that I need? If it isn't then don't hand over money.
INVESTIGATE	If you are being sold a product, check that the company is who they say they are.

BIG SCAMS

TICKETING SCAMS

Getting tickets to see your favourite band, football team, popular theatre production or festival can be very difficult as tickets can sell out quickly. Scammers are taking advantage of this by tempting you to buy tickets that do not exist or are fake. Scammers set up websites offering tickets that they do not have access to and cannot provide but are happy to take payment for.

What you should know

- ⚠ The scammer's website will offer tickets to events that are sold out or tickets that have not gone on sale yet.
- ⚠ You may receive the tickets you have paid for but when you arrive at the event you find out they are fake or have been reported as lost or stolen and are therefore invalid.
- ⚠ Scammers may tell you a representative will meet you at the event with your tickets and they do not arrive.
- ⚠ Paying for tickets using your credit card offers protection under the Consumer Credit Act if you are scammed.
- ⚠ Checking online may provide details of any negative reviews of the website you intend to use.
- ⚠ Remember the only way to avoid being scammed is to buy tickets from the promoter, the venue box office, a reputable ticket exchange site or an official agent.
- ⚠ If a website shows the STAR – Society of Ticket Agents and Retailers logo then check that they really are members by contacting STAR directly. *Contact details are available at the back of this book.*

STAR STAR.ORG.UK SECURE TICKETS *from* AUTHORISED RETAILERS™

BIG SCAMS

ONLINE SHOPPING AND AUCTION FRAUD

Online shopping is becoming more and more popular. It can save time and effort and gives you a wide choice of goods from around the world. Scammers use online shopping scams because they can hide their identity using the internet.

What you should know

- ⚠ Scammers will often try to encourage you to leave a legitimate site to complete a sale. If you do this you could lose any payment protection the legitimate auction site offers its users.
- ⚠ It's unlikely for luxury or designer goods to be associated with the words 'cheap' or 'bargain'. Scammers will often over emphasis words such as 'genuine' and 'authentic'.
- ⚠ Never pay for a vehicle without viewing it, and relevant documentation, in person first. You may be offered a low price or discount to make payment prior to seeing the car or it being delivered – don't.
- ⚠ Just because a website says its .co.uk doesn't mean it is based in the UK. Check the address of the company and the phone number.
- ⚠ Beware when selling items online. Scammers can enter a very low bid and then using another name enter an extremely high bid. Just before bidding closes the high bidder will withdraw leaving the scammers low bid to win.
- ⚠ Research the sellers and any other bidders selling history.

BE SUSPICIOUS

BIG SCAMS

REMEMBER	Paying by credit card offers greater protection than with other methods.
CAUTION	Check the payment page is secure. A padlock is in the browser, the web address starts 'https:/'s' stands for secure.
THINK	Why am I being encouraged to buy off site?
INVESTIGATE	Check the sellers terms and conditions including privacy and returns policy.

BIG SCAMS

INTERNET SCAMS

Many internet scams take place without the victim even noticing. Scammers may attempt to put programs on your computer that can steal, wipe or lock your data. To prevent this ensure you have anti-virus software and a firewall installed on your computer and keep it up to date. If you are aware of the following precautions and apply common sense then you should be able to prevent yourself from becoming a victim.

What you should know

⚠ Scammers can use the internet to promote fraud through unsolicited or junk emails known as spam. Delete the email otherwise the scammer will continue to send you more and more emails from lots of different addresses.

⚠ Any email you receive that comes from an unknown sender is likely to be spam especially if it is not addressed to you personally and promises you some gain.

⚠ If you receive an email with an attachment from someone you know but it is not the usual sort of message you get from them DO NOT open the attachment. Speak to the person who is supposed to have sent it to confirm its origin. It may have been infected with a virus and forwarded through their address book.

⚠ Online market places can be a lot of fun and can save you money but they are also used by scammers. Scammers will try to steer you away from online sites and request that you use unusual payment methods e.g. money transfer agents or Emoney, a digital equivalent of cash.

⚠ The most common scams at the moment are for concert and event tickets, apartments, residential and holiday lettings, dating and romance and vehicles for sale or hire (especially if hire vehicles are to be delivered to you). Adverts and websites can be very sophisticated so do some research to ensure everything makes sense. Always consider your personal safety when meeting anyone you have met on the internet.

INTERNET SCAMS

- ⚠ Be careful of bogus official looking websites, claiming to assist in applying for passports, visas and driving licences.
- ⚠ There are lots of ways scammers gain personal and/or financial information from victims – e.g. Phishing (unsolicited email purporting to be from a legitimate company requiring personal details), Vishing (voice over cold calling purporting to be from a legitimate company requiring personal details) and Spear Phishing (type of **phishing** scam that focuses on an individual or department within an organisation, addressed from someone within the company in a position of trust). Using these methods scammers request information such as **login** details and **passwords**.
- ⚠ Never give your personal or financial details to anyone unless you know and trust who you are giving them to.

BIG SCAMS

REMEMBER	Delete all messages without reading them if they are from somebody you do not know. If you open it by mistake and it has an attachment, do not open that attachment. It may be a virus.
CAUTION	Don't reply to spam emails even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Ensure you have up-to-date anti-virus and firewall software.
THINK	Why is this person contacting me? Be wary of any request to use an unusual payment method.
INVESTIGATE	Make sure the sites are genuine as some business websites can be copied, cloned or redirected.

INTERNET SCAMS

BIG SCAMS

FREQUENT SCAMMING TOOLS

Scammers often use one or more of the following to help them commit fraud and hide their true identity.

Money Transfer Agents

Using a money transfer service is a way to send money to people that you know and trust. Money transfer agents offer fast, convenient and reliable options for customers to send and receive money worldwide.

However, they are often used by scammers in order to commit many types of fraud such as advance fee, identity theft, investments and mass market fraud to name a few.

WHILST THE SENDER OF THE MONEY HAS TO PRODUCE IDENTITY DOCUMENTS, THOSE THAT COLLECT THE MONEY DO NOT. This is why scammers will often try to get you to send them money using a money transfer agent. This method enables them to hide their identity.

Ensure you know who the individual is you are dealing with before providing them with any reference numbers they require to collect the money you have deposited.

You should:

- ⚠ Never let a scammer educate you on how a money transfer service or cash voucher systems works – only take advice from the money transfer or cash voucher company.
- ⚠ Read the warnings on money transfer documents. The information is there to protect you.
- ⚠ Do not pay for items bought online, including auction sites using a money transfer agent. Money transfer agents are not responsible for the satisfactory receipt of goods or services paid for by means of a money transfer.
- ⚠ Never share details of a money transfer with anyone else to prove the availability of funds. Doing so may enable the money transfer to be paid to that third party. This is known as a 'Proof of Funds' fraud.

Virtual Offices

A virtual office is an address where any person or business wishing to use an alternative address to their own can be registered. They may never attend the address and can have all mail delivered to the virtual address redirected.

You may think you are dealing with a well established, professional individual or business because of a prestigious 'virtual office' address. However, the reality can be very different.

The majority of businesses using 'virtual offices' are honest and legitimate. However, scammers often use a virtual office address instead of their own home or business address in order to hide their true identity. Often scammers use false ID to obtain the virtual office facilities.

If you see a website that has an address on it be aware that the address could well be a virtual office address and the company does not operate from it. Victims of scams have been known to attend addresses on correspondence from companies and are surprised and dismayed to find that the office is a virtual office.

Telephone Numbers

A handful of telecommunications companies are able to provide non-geographical telephone numbers, e.g. 0800 or 0845 numbers, and premium rate numbers to businesses or individuals.

Depending on the type of service paid for the customer does not have to provide identification. Scammers will often use these numbers and have them diverted to unregistered pay-as-you go mobile phone numbers, or to a separate telephone answering service making tracing them difficult.

You should not rely on the appearance of a telephone number to tell you what sort of number it is. For example '0208' is usually a London number and '07952' a UK mobile number. However, telephone numbers can be purchased by scammers to trick you into believing they are legitimate and based where you think they are.

Software has also become available that enables scammers to have any number they wish to appear on the caller ID screen on your phone. This method know as 'spoofing' allows the scammer to appear to be calling from a legitimate number linked to a person or company when in fact they are not.

Always be cautious about the person's identity when speaking to people you do not know on the telephone.

Be aware that if the scammer gives out a telephone number that phone number cannot always be traced and the user identified.

BIG SCAMS

FRAUD IS NOT A VICTIMLESS CRIME

Scams DO happen

Romance/Dating Fraud

A 50 year old female lost £40,000 after corresponding with a suspect she met via a dating website. The suspect claimed he was an officer in the armed forces and was serving overseas. His profile showed a handsome male in uniform. The suspect initially engaged with the victim through her profile on the dating site before encouraging her to communicate with him through personal email and telephone. The suspect built a rapport with the victim and she believed they were in a relationship.

The suspect made a number of arrangements to meet the victim but on each occasion he cancelled stating he could not meet her due to work commitments.

Over a period of time the suspect confided in the victim that he wanted to discharge himself from the army so they could be together. He informed her that he did not have the funds to pay to be discharged and was able to persuade the victim to send him £40,000 which she believed was to be used by the suspect to buy himself out of the army.

The suspect continued to ask for more money and on being told by the victim she had sent him all the money she had the suspect stopped all contact. It was at this time the victim realised she had been scammed. Police enquiries confirmed the victim had sent the funds to Africa and that emails sent by the suspect had originated in Africa when the suspect claimed to be serving in the Middle East. It was also found that the photograph of the suspect on the website had been taken from the social media profile of another person.

Investment Fraud

A 75 year old victim was contacted by telephone by a company offering investment in fine wine. Good returns were offered and the victim was led to believe that the wine was available at below market value. The company sent an attractive brochure to the victim and had a well designed web site. The investment company was also listed with Companies House.

The victim invested £12,000 and was provided with paperwork regarding the purchase. He was informed the wine would be held in bonded storage for tax purpose so never actually saw what he had invested in.

On trying to sell the wine via the investment company the victim was continually advised to maintain the investment for increased returns. He eventually contacted the bonded warehouse and found that no wine existed and he had been the victim of a scam.

Police were informed and a number of suspects involved in the operation of the company were arrested and charged with fraud and money laundering offences. They received significant prison sentences on conviction.

Holiday Fraud

A victim lost £3000 after attempting to book a holiday villa via the internet. He had contacted a reputable website via email and was in the process of confirming his booking. He received an email purporting from another member of staff at the holiday company which stated he would receive a discount if he paid for the villa directly to its owner. Wanting to take advantage of this offer the victim paid for the accommodation directly into a bank account provided by email.

The victim became concerned when he did not receive a confirmation from the holiday company and contacted them via the telephone number on their website. He was informed that the company had no record of his booking and their systems stated he had emailed the company to say he was not interested in any of their properties.

It was established that the victim's email account had been hacked and the suspects had discovered the victim was looking to rent a holiday property. The suspect had then sent emails to the victim from a similar email address to that of the holiday company persuading him to pay funds into a fraudulently opened bank account.

The victim was unable to reclaim the funds he had paid as he had made a bank to bank transfer.

Police were unable to locate any suspects as unregistered computers were used by the suspect and the person opening the fraudulent bank account could not be identified.

BIG SCAMS

HANDY HINTS TO PROTECT YOURSELF

Protect your identity

- Only give out your personal details when absolutely necessary and when you trust the person you are talking to.
- Destroy personal information. Make sure you shred all documents, old credit and debit cards and anything else with personal details on.
- Treat personal details like you would money. Don't leave them lying around for others to see and take.
- Be wary of who you give your personal details to in the street (e.g. charities, products, competitions etc). Do not sign up for anything until you have researched the company or charity.

Money matters

- Never send money to anyone you don't know.
- Do not send any money or pay fees to claim prizes or lottery winnings.
- Responding to jobs adverts asking to simply use your bank account to transfer money for somebody could be a front for money laundering activity. Money laundering is a serious criminal offence and can carry a prison sentence of up to fourteen years.
- Avoid transferring or sending any refunds or overpayments back to anyone you do not know.

The face-to-face approach

- If anyone comes to your door, make sure you ask for identification. You DO NOT have to let them in and they must leave if you tell them to.
- If you are interested in what a door-to-door salesman is offering, do not agree to buy anything there and then. Take time to find out about their business. Get two or three quotes from different businesses.
- Contact Citizens Advice Consumer Service if you are unsure about a trader that comes to your door.

Telephone business

⚠ If you receive a phone call from someone you don't know, always ask for the name of the person you are speaking to and who they represent. Verify this information by calling the company's head office yourself on a different phone line in case the caller is holding the line open.

⚠ Never give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.

⚠ It is best not to respond to text messages or missed calls that come from numbers you do not recognise. Be especially wary of phone numbers you do not know. They may charge you higher rates if you answer them and can turn out to be very expensive.

⚠ Never assume that someone is who they say they are just because the number on your caller display matches that of the organisation you know. Scammers can clone telephone numbers of organisations they want to impersonate and make the number appear on your caller ID display.

Email offers

⚠ Never reply to spam emails, even to stop them. Often this just serves to verify to scammers that the address is active. The best course of action is to delete any suspicious emails without opening them.

BE SUSPICIOUS

- Legitimate banks and financial institutions will never ask you to click on a link in an email to access your account and will never ask you for your PIN number.
- Never call a telephone number or trust any contact details in a spam email.

Internet business

- Install software that protects your computer from viruses and unwanted programs and make sure it is kept up to date. If you are unsure how to do this seek the help of a computer professional.

General

Be suspicious and remember:

- If it sounds too good to be true it probably is.
- Be wary of people or companies using virtual offices, money transfer agents and other new and unusual methods of payment – e.g. Emoney, a digital equivalent of cash that can be stored on an electronic device.
- Be aware that whilst banks are normally good at ensuring their customers are who they say they are, scammers can and do open up bank accounts using false details.
- Be aware that scammers can be clever. They will have done their homework and will often know huge amounts of information about people they target. Often they are very organised and capable.
- They will try to hide their true identity by using a variety of methods.

BIG SCAMS

WHAT TO DO IF YOU GET SCAMMED

GET HELP AND REPORT A SCAM

If you think you have uncovered a scam, have been targeted by a scam or fallen victim, there are many authorities you can contact for advice or to make a report.

Reporting crime, including fraud, is important. If you don't tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim of a scam or an attempted scam, however minor, there may be hundreds or thousands of others in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

Reporting fraud

In the Metropolitan Police area as of April 2013, all fraud should be reported directly to Action Fraud.

Action Fraud
Reporting online: www.actionfraud.org.uk
Telephone reporting: 0300 123 2040

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Unless

- ⚠ A crime is in progress or about to be committed.
- ⚠ The suspect is known or can be easily identified.
- ⚠ The crime involves a vulnerable victim.

If this is the case you should contact police directly either by dialing 999 in an emergency, dialing 101 in a non-emergency or visiting your local police station.

If you have any information on any crime and you would prefer not to speak to police, you can call Crimestoppers anonymously on 0800 555 111 or visit www.crimestoppers-uk.org Crimestoppers is an independent charity.

OTHER CONTACTS

ABTA – Association of British Travel Agents

The largest travel trade association in the UK with over 1,200 members. ABTA conducts rigorous checks on its members to ensure they are financially solvent as well as background checks on all company directors of its members. All ABTA members must follow ABTA's strict Code of Conduct, if they breach this code they can be fined or have their membership terminated.

If you have a complaint against an ABTA member or want to check that a company is an ABTA member go to www.abta.com or call 020 3117 5599

Action on Elder Abuse

AEA are a national charity working to protect and prevent the abuse of vulnerable older adults.

Tel: 020 8835 9280
Helpline: 0808 808 8141 (Mon to Fri)
Web: www.elderabuse.org.uk

Age UK

Provide companionship, advice and support for millions of people in later life. For free, confidential, information and advice call their national advice line on 0800 169 6565 or visit www.ageuk.org.uk

Alzheimers Society

A National based charity providing advice and support for people affected by dementia.

Tel: 0300 222 1122
Web: www.alzheimers.org.uk

Citizens Advice Bureaux (CAB)

Citizens Advice Bureaux can help you solve your legal, money and other problems by providing free, independent and confidential advice.

For online information and to find your local CAB see www.adviceguide.org.uk or look under C in the phone book.

Tel: 08444 111 444
Citizens Advice Consumer Helpline: 03454 04 05 06
Web: www.citizensadvice.org.uk

Financial Conduct Authority (FCA)

Provides information on how to find and choose a financial advisor and can confirm whether your advisor is authorised. It also produces a wide range of materials on finance-related matters.

Consumer Helpline: 0845 606 1234
Web: www.fsa.gov.uk

Financial Fraud Action UK (FFA)

The FFA is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Their membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK.

They provide a forum for their members to work together on issues relating to financial fraud. Their primary function is to facilitate collaborative activity between industry participants and with other partners committed to fighting fraud.

Web: www.financialfraudaction.org.uk

Insolvency Service

The Insolvency Service is an Executive Agency of the Department of Business, Innovation and Skills (BIS). The Company Investigations team within the Insolvency Service has the power to investigate limited companies where information received suggests corporate abuse; this may include serious misconduct, fraud, scams or sharp practice in the way a company operates.

To complain about a limited company that is still trading:

Tel: 0845 601 3546
Post: Intelligence Hub
Investigation and Enforcement Services
Insolvency Service
3rd Floor Cannon House
18 Priory Queensway
Birmingham B4 6FD

Email: intelligence.live@insolvency.gsi.gov.uk
Web: www.gov.uk/government/organisations/insolvency-service

Office of the Public Guardian (OPG)

The OPG is responsible for protecting people who no longer have the capacity to make certain decisions themselves. It does this through:

- The supervision of Deputies appointed by the Court of Protection (CoP).
- The registration of Enduring Powers of Attorney (EPAs) and Lasting Powers of Attorney (LPAs).
- Maintaining a register of Deputies, Enduring Powers of Attorney and Lasting Powers of Attorney.
- Investigating allegations of abuse by Court appointed Deputies or Attorneys acting under a registered EPA or LPA.
- Policy ownership of the MCA and the Code.

Office of the Public Guardian
PO Box 16185 Birmingham B2 2WH
Enquiry Line: 0300 456 0300

Online Dating Association (ODA)

With more and more people meeting online the ODA was been set up to maintain standards across the industry and reassure members of the public that each provider is working to achieve the highest standards.

Dating services that have ODA membership go through a test of their commitment to the industry's Code of Practice. They are committed to this set of standards and to providing users with advice, guidance and support in the event of any problems.

People should look for the ODA logo on a site as assurance that the service provider is part of the self-regulatory community.

Web: www.onlinedatingassociation.org.uk
Correspondence Address:
1 Bromley Lane
Chislehurst
Bromley
BR7 6LH

JUST REMEMBER:
IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.

Royal Mail scam mail helpline

What can I do about scam mail?

Scams can come to you by phone, email or post. There are many different types of scams, such as fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams and pyramid selling, to name just a few.
It's important to note there is a difference between scam mail and legitimate mail sent by companies to advertise lawful services or the sale of genuine goods. Scam mail is sent for the sole intention of obtaining money through deception and/or fraud.

Royal Mail is bound by the Universal Service Obligation and is required by law to deliver all mail entrusted to it. However, they are determined to do all they can to prevent scam mail entering the postal system with the help of their customers. They want to know about potentially fraudulent mail so they can work with the relevant authorities who can then investigate and take action.

What to do

If you think you or a family member is receiving scam mail, you can report it to Royal Mail.

If you have received items of mail you believe to be from fraudsters please send them, with a covering letter to:

Freepost Scam Mail
Scam Mail
PO Box 797
EXETER
EX1 9UN

You can also email Royal mail at scam.mail@royalmail.com or report your concerns by calling 08456 113 413.
Royal mail will send you a scam mail report form for completion together with a prepaid addressed envelope in which to return the form with examples of the scam mail received.

If you are moving home

To reduce the risk of identity fraud you should use Royal Mail's Redirection service to redirect mail from your old address to your new address for at least a year.
If you hold power of attorney for somebody who you believe is a victim or vulnerable to being a victim of scam mail you can apply of their behalf for a Redirection of mail at a Post Office branch or by post.

SCIE

The Social Care Institute for Excellence (SCIE) improves the lives of people who use care services by sharing knowledge about what works. They are an independent charity working with adults, families and children's social care and social work services across the UK. They also work closely with related services such as health care and housing.

For general enquiries:

Tel: 020 7024 7650
Email: info@scie.org.uk
Web: www.scie.org.uk

Society of Ticket Agents and Retailers

STAR is the leading self-regulatory body for the entertainment ticketing industry across the United Kingdom, it offers general advice and information on ticket buying and provides a dispute resolution service for customers who have an unresolved problem with their purchase from a STAR member.

Society of Ticket Agents and Retailers
PO Box 708
St Leonard's Place, YORK YO1 0GT
Tel: 01904 234737
Email: info@star.org.uk
Web: www.star.org.uk

The Mailing Preference Service (MPS)

is a free service enabling consumers to have their names and home addresses in the UK removed from mailing lists used by the industry. It is actively supported by Royal Mail, all directly involved trade associations and the Information Commissioners Office. It will take up to 4 months for the service to have full effect although you should notice a reduction in mail during this period.

To Register for the Mail Preference Service:

Tel: 0207 2913300 or
Web: www.mpsonline.org.uk

The Silver Line

The Silver Line is the only free confidential helpline providing information, friendship and advice to older people, open 24 hours a day, every day of the year.

The Silver Line Helpline provides three functions to support older people:

- a sign-posting service to link them into the many, varied services that exist around the country
- a befriending service to combat loneliness
- a means of empowering those who may

be suffering abuse and neglect, if appropriate to transfer them to specialist services to protect them from harm

Need help? Call ANYTIME on:
0800 470 80 90
Web: www.thesilverline.org.uk

The 'Opt Out' Services
Companies may pass on your personal details to other companies unless you 'opt out'. Whether you are purchasing goods or obtaining a loyalty card you should carefully read all the terms and conditions to ensure your details are not forwarded without your consent.

To Opt Out from receiving Door to Door, unaddressed mail, delivered by Royal Mail you may contact Royal Mail.

Tel: 08457 950 950
Email: optout@royalmail.com

NB - Royal Mail are still legally obliged to deliver all addressed mail, which includes mail that is addressed "To the Occupier" (or with any other generic recipient information), as well as mail that is personally addressed to you by name.

Opting out from other unaddressed mail deliveries.

To opt-out from deliveries from other unaddressed mail distributors you may wish to register with the 'Your Choice' preference scheme run by the Direct Marketing Association. They can be contacted at:

'Your Choice' Preference Scheme
Direct Marketing Association (UK) Ltd
DMA House
70, Margaret Street,
London W1W 8SS
Telephone: 020 7291 3300
Fax: 020 7323 4165
Email: yourchoice@dma.org.uk

The Telephone Preference Service (TPS)
is a free service. It is the official central opt out register on which you can record your preference not to receive unsolicited sales or marketing calls. It is a legal requirement that all organisations (including charities, voluntary organisations and political parties) do not make such calls to numbers registered with the TPS unless they have your consent to do so.

To register free with the Telephone Preference Service:

Tel: 0800 398893 or
Web: www.tpsonline.org.uk

Think Jessica

If you are a victim of Mass Market Fraud then you can contact Think Jessica for advice.
Email: advice@thinkjessica.com

If you would like a Think Jessica information pack about scam mail (includes DVD). Please send a cheque or postal order for £5.00 (to cover production and postage).

Think Jessica
PO Box 4244, Chesterfield S44 9AS

REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to **reduce the damage** and avoid becoming a target again.

The quicker you act, the more chance you have of reducing your losses.

Report a scam

By reporting the scam to Action Fraud, Police or Trading Standards, we will be able to warn other people about the scam and minimise the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across.

Scammers are quick to identify new ways of conning people out of their money. Be aware that any new scheme or initiative will quickly be targeted.

Finally, remember that this booklet does not contain all the answers but to avoid being a victim you need to be aware that someone who is not suspicious and has a trusting nature is a prime target for a scammer.

Be suspicious and remember if it sounds too good to be true it probably is!

An audio, 'easy read' and E-version of the original booklet is available on our website **www.met.police.uk/fraudalert**

If you are a member of the public or organisation and reside within the Metropolitan Police Area then to request further copies of this booklet or to obtain an audio or easy read version, contact FALCON Prevention, Metropolitan Police Service on **020 7230 1228** or email **Sterling@met.pnn.police.uk**

FALCON Prevention has provided other police forces with the necessary details to print further copies at their own cost. If you reside outside of the Metropolitan Police Area then contact your local police force who may be printing their own version.

The Metropolitan Police Service would like to thank the following for their time and effort in assisting with the third edition of this booklet:

Australian Competition and Consumer Commission

Barclays Bank PLC

C Hoare & Co

Financial Fraud Action UK

Royal Bank of Scotland PLC

Worldpay

FALCON
FRAUD AND LINKED CRIME ONLINE

Published by the Metropolitan Police Service