

Operation Sterling:

Prevention Toolkit

**"An ounce of prevention is better than
a pound of cure"**

circa 13th Century

This document aims to provide a range of practical advice to reduce vulnerability to fraud. It is only an advice document, not a list of solutions to problems

Under the Fraud Act 2006, fraud can be committed in three ways, namely by; false representation, failing to disclose information and abuse of position.

Many other common terms are used to describe fraud – for example scam, con, and deception. Other specific frauds have their own names, for example Identity Fraud and advanced fee fraud.

Fraud is often viewed as a victimless crime but this is incorrect. Individuals often suffer financial loss, distress and inconvenience. Even losses to credit card and insurance companies are passed on to their customers in increased interest rates and premiums.

The Metropolitan Police Sterling Prevention Team works with a very wide range of public and private sector organisations in order to 'design out' fraud and other economic crime, providing practical crime prevention advice to organisations and individuals.

Other agencies such as Trading Standards and the Office of Fair Trading have a remit to deal with bad business practice and disputes over contracts or other transactions. A key partner is the Scambusters Team at the OFT. Other Sterling activities include participation in the National Identity Fraud Prevention Week. and the London Fraud Forum.

A 'scam' is usually viewed as low in value, but there may be a high number of offences. Taken individually, the effect of low value frauds may be viewed as minor and of little consequence, however, the effect on individuals and the gain to the criminal enterprise can be very significant.

Remember our top crime prevention bullet points.

- Treat all callers as bogus until you can satisfy yourself that they are genuine.
- Fraudsters are very plausible and are skilled in persuasion.
- You cannot win a prize in a competition that you have not entered.
- Only send money to a person who you know and trust.
- If it appears too good to be true then it invariably is.

Advice Sections:

1. Identity Fraud
2. Mass Marketing Fraud.
3. Doorstep Crime and Bogus Callers.
4. Intellectual Property Rights, Trademarks and Counterfeiting.
5. Phone Calls and Call Costs.
6. Marketing phone calls and Junk mail.
7. Vulnerable Groups and Elder Abuse.
8. The Internet and e-Mail.
9. Money Transfer
10. Vehicle Buying and Selling, Shipping and Escrow fraud.
11. Allegations of Crime, Complaints and other reports.
12. Sources of Information.



Working together for a safer London

ECONOMIC AND SPECIALIST CRIME

1) Identity Fraud.

Identity Fraud has become a major issue and concern to all. Many frauds involve the unauthorised use of other peoples' cheques, credit cards or other documents.

The taking over of a persons' identity is becoming more prevalent, enabled by the availability of information about other people, especially over the Internet.

The most common form of Identity Fraud is the use of debit and credit card details. Since the introduction of 'Chip and PIN' cards, the problem has shifted to 'Card Not Present' transactions.

'Chip and PIN' and Internet transactions are usually safer than other methods of payment, particularly when paying with a credit card. Giving card details over the phone or handing a card to a person gives a greater opportunity to record the card details, signature and security number from the back of the card.

There are a number of things an individual can do to help protect their personal data, e.g., protect your PIN details.

Electoral Roll (Voters Register)

In order to avoid your electoral register details being publicly available on the web and to marketing companies, tick the box on your registration form to opt out from the 'edited' register.

Credit Reference Agencies

These agencies hold credit and other information. They issue alerts to inform their customers somebody may be mis-using their identity.

Callcredit Plc 08700 60 14 14
www.callcredit.co.uk

Equifax Ltd 08700 100 583
www.equifax.co.uk

Experian Ltd 08702 416 212
www.experian.co.uk

Victims of Identity Fraud are advised to ensure that their details are 'Protectively Registered' with CIFAS. For a small fee, CIFAS will notify all member companies and credit reference agencies that your personal data has been compromised.
<http://www.cifas.org.uk/>.

CIFAS Protective Registration Service:
0870 010 2091 e-mail
protective.registration.uk@equifax.com

Chip and Signature cards:

Under the Banking Code issued by the British Banking Association, all issuers of debit and credit cards must offer an alternative to 'Chip and PIN' cards to people who are unable to use a PIN due to disability or medical condition.

- Chip and signature cards look and work just like chip and PIN cards. The only difference is that when you put your card into a PIN pad, instead of being prompted to provide a PIN, the technology will recognise that no PIN is needed and print out a receipt for the assistant to give you to sign.
- All the retailer needs to do is to follow the instructions on the terminal screen – it will prompt the shop assistant to accept your signature rather than a PIN. All retailers will have procedures in place to ensure they accept cards without a PIN.
- If you have trouble remembering your PIN and need to write it down or tell someone else the number, contact your bank to get a chip and signature card instead.

This advice is provided by the British Banking Association and APACS, who are now known as the UK Cards Association.

The Banking Code:
www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf

UK Cards Association. Payments & Accessibility guide.
www.apacs.org.uk/resources_publications/documents/081208_Paymentsandaccessibility_v3_1.pdf

2) Mass Marketing Fraud.

There is often a fine line between what is a crime and a sharp business practice. A scam is a scheme designed to con you out of your cash.

We are all potential victims of scams. If you let down your guard and think that you won't be fooled, then you too could become a victim.

Fraudsters are becoming more sophisticated. They are persuasive and plausible in their efforts to get us to part with our money. Deceptive premium rate competition scams, bogus sweepstakes and lotteries, get-rich quick schemes and fake health cures are some of the favoured means of separating the unwary from their money. The number and variety of scams keeps on growing.

The OFT website is <http://www.of.gov.uk/> and the Scambuster home page is <http://www.of.gov.uk/Consumer/Scams/default.htm>

Advice leaflets and a DVD are available on the website where copies can be ordered.

How to recognise a fraud –

If it is too good to be true it usually is!

THE CON MAN

How Scam Artists succeed - They will:

- Catch you unprepared, contacting you without invitation by phone, email, post or even in person.
- Appear pleasant, well spoken and kind (on the phone or at your door) and want you to think they are your friend. They may produce professional leaflets and letters to substantiate their story.
- Be persistent and persuasive.
- Pressure you into making a decision
- Ask you to send money before you receive anything promised.

New frauds from the UK and overseas appear every day - so it's important to know how to spot them. You should view all propositions objectively and be circumspect.

THE PITCH

They may offer you something for nothing or too tempting to ignore- such as:

- You've won a major prize in a draw or a lottery (even though you had not entered one),
- An exclusive entry to a scheme that's a surefire way to make money,
- A way to earn easy money by helping them transfer millions out of another country,
- The chance to join an investment scheme that offers substantial returns on your investment.

There are hundreds of examples but we can all protect ourselves by being sceptical. Ask yourself is it likely that someone you don't know, who has contacted you out of the blue, will give you something for nothing ? The answer is NO!

THE STING

They'll ask you to:

- Send money up front for administration fees, taxes or other associated costs. The list is endless but it's always a ruse to get you to give them money
- Give them your bank, credit card or other personal details.
- Ring an expensive premium rate phone number. (See Phone Calls section below).
- Buy something to get your prize.

They will lie to you and give good reasons why you should do what they say. They will give you plausible explanations.

Don't send any money or give any personal details to anyone until you've checked that they are genuine. Always talk to a professional, family member or friend if you are unsure.

Other things to look out for which should increase your suspicion.

- They ask you to send money straight away
- They give you a PO box number or an address that will act as a forwarding point for any correspondence that you may send.
- They ask you not to tell anyone about the deal.

3) Doorstep Crime – dealing with bogus callers.

Doorstep Crime is the name given to offences committed by people who call door-to-door 'cold calling' to sell goods or offer repairs, gardening or other services. At best, the caller may be an unwanted salesperson, at worst a burglar seeking an easy way into the premises or a fraudster seeking to take money or defraud the occupier.

The Doorstep Selling Regulations, which came into force in 2008 apply to most things that are sold door to door and criminal offences are committed by persons who contravene these regulations.

Most companies do not usually engage in 'Doorstep Selling'. Companies that do, often employ high pressure selling techniques that can be very intimidating for the elderly and vulnerable.

Trading Standards often work with local police and will set up 'No Cold Calling Zones'. These areas have street signs of a similar size to Neighbourhood Watch signs and although they are not enforceable they enable householders to inform potential bogus officials to 'go away'.

Trading Standards officers are also working with local banks and building societies educating staff to spot unusual withdrawals, such as the elderly paying excessive amounts for building work.

The best advice is to assume that the caller is a 'Bogus Caller'.

Use a chain when answering the door, and thoroughly check their identification by contacting the company or organisation if necessary.

If they are genuine they will not mind.

A successful prosecution of a 'Roofer' came about as a result of Trading Standards officers patrolling an area and seeing some work being done. The elderly victim was about to pay several thousand pounds for a small job on his roof. The offenders had made £448,000 from their victims. SCD6 officers assisted in the prosecution and confiscated the proceeds of crime from the offenders.

4) Intellectual Property Rights, Trademarks and Counterfeiting.

Intellectual Property Rights (IP), Trademark and Counterfeiting are crimes that often come to the attention of police and Trading Standards.

Again the losses caused by such infringements is not a victimless crime, it has a direct consequence to employment and creativity in the UK economy.

Counterfeit goods is becoming an increasing area of Trading Standards activity and practically anything, from soft drinks, to complete motorcycles are being counterfeited.

There are particular problems with DVD's and cigarettes being openly on sale in town centres and elsewhere. These are parts of organized criminal networks with links to other crimes such as human trafficking.

Counterfeit cigarettes and DVD's are easily detectable in the way that they are usually sold. Local Trading Standards departments would handle prosecution of street sellers. Other items, such as clothing, are more difficult to identify and require specialist knowledge. These are best dealt with by pre-planned joint operations in consultation with your local Trading Standards Office.

The Federation Against Copyright Theft can be contacted on 020 8568 6646. www.fact-uk.org.uk

The Federation Against Software Theft (FAST) deals with the pirating of computer games and software. www.fastiis.org/

The BPI deals with the counterfeiting of Music CD's and unauthorised downloads. www.bpi.co.uk

The Intellectual Property Office (formerly the Patent Office). www.ipo.gov.uk

5) Phone Calls and Call Costs.

Unwanted phone calls can be much more than a nuisance and phone calls can cost far more than expected.

Do not assume that a landline number identifies where the phone is. Fraudsters will use call redirect companies to direct calls to other countries or mobile phones.

Call costs vary significantly according to the phone company and whether the call is to a mobile or landline. The important thing is to know what tariff or price plan you are on and the cost of calls.

Most price plans have a number of 'inclusive' calls but these are only to numbers beginning 01, 02 and the new 03 non-geographic numbers.

0800 numbers are 'freephone' numbers on land lines only - most mobile operators charge your "normal" rate to call these numbers which can be 50p per minute.

0845, 0870 and other numbers beginning 084 and 087 are 'revenue sharing' non-geographic numbers most commonly used by call centres anywhere in the world. The calls can cost as much as 10p per minute, with the company taking a share of the cost.

070 numbers were designated as business numbers allowing calls to connect to people on the move. They are however, used frequently by fraudsters to avoid detection.

Calls to 090 numbers involve a payment, this can be up to £1.50 per minute. Many prize competitions ask for a 'call back' on these numbers at great cost to the unwary. The competition may be completely legal.

Check your bills regularly and understand the charges.

Alternative numbers to 0870, 0845 and other non-geographic numbers can be found on the web site: www.saynoto0870.co.uk.

Further information can be found at the Phone Pay Plus and OFCOM web sites www.phonepayplus.org.uk www.ofcom.org.uk/consumeradvice

6) Marketing phone calls and Junk mail.

Marketing phone calls, and unsolicited mail are legitimate marketing practices for many companies. However, silent phone calls and 'junk' mail can be misleading, a nuisance and distressing.

The Direct Marketing Association (DMA) is the largest trade association for the marketing and communications sector.

The DMA is answerable to the Direct Marketing Commission (DMC) who have power to enforce standards across the advertising industry. The UK DMA operates preference services to block unwanted mail, telephone calls and faxes.

Silent phone calls often happen when a computer has dialled several phone numbers. Only the first person to answer is spoken to and the remainder get a 'silent call'. Often the call will be a competition or offer but it may be a message to call a premium rate number.

Always be very careful about disclosing security information to people that have called you. Always take their details and ring them back on the number that you have for them. Use the number on your bill or card.

The procedure to register for the Telephone Preference Service is to call 0800 398893. See www.tpsonline.org.uk The fax preference service is on 020 7291 3330 or at www.tpsonline.org.uk/fps/

Unsolicited mail should be treated with caution and never reply to something that you believe or suspect to be a fraud. Contact genuine organisations and ask to be removed from their mailing lists. When filling out a form, find out how the information is used. Consider opting out.

Register for the Mail Preference Service online at <http://www.mpsonline.org.uk>, or call 0207 2913300.

The Royal Mail delivers letters addressed to 'the occupier'. These can be opted out of by emailing optout@royalmail.com or telephoning 08457 950 950.

The Metropolitan Police non-urgent call number is now 0300 123 1212.

7) Vulnerable Groups and Elder Abuse.

Those less able to look after themselves, can often be subject to financial exploitation as well as physical attack.

Unfortunately not only strangers but people close to members of vulnerable groups such as relatives, friends and carers, have the ability to carry out physical, mental and financial abuse. Even people acting with a power of attorney have been guilty of fraud.

The Office of the Public Guardian (OPG) oversees Powers of Attorney and Court of Protection Orders. These are formal orders that can be put in place in advance of or after a person lacks the capability to make decisions or manage their affairs.

The OPG guidance can be found at: www.publicguardian.gov.uk/decisions/decisions.htm

However, many people require help in managing their day-to-day activities – talking on the phone, understanding letters and other correspondence for example.

Often, the Data Protection Act (DPA) is cited as the reason for only dealing directly with the account holder. The Information Commissioner's Office, (ICO) regulates data protection and urges a common sense approach when dealing with people acting on behalf of another, for example, relatives of the elderly. Whilst an organisation may not wish to discuss or disclose information about an individual, there is nothing to stop them receiving and evaluating information then taking appropriate action.

Under the DPA, organisations do have a responsibility to ensure that their data is accurate and up to date. If a relative of a customer wants their elderly relative removed from a mailing list because they are now in a nursing home, the records should be updated.

The Information Commissioner has issued a guidance note "Providing Personal Account Information to A Third Party" which can be found: on their web site www.ico.gov.uk

8) The Internet, Web Sites and e-Mail.

Use of the Internet and email is something that is taken for granted these days. There are many sources of advice. Get Safe On Line www.getsafeonline.org is an impartial site.

Fraud, ID theft and scams over the Internet rely on financial information being sent or obtained by criminals. This may be personal information, a payment or technical attacks on home computers.

Lured into a false sense of security, victims forget that they are not dealing face to face with the other party – they believe what they see is true without reservation or caution. It is important for individuals to question whom they are dealing with and to be objective.

Most Internet users are aware of "phishing" emails. These are requests to supply security information following some crisis or another. A new threat are emails that appear to be marketing, (known as spear phishing emails). The links in the email take the user to a bogus web site. The user may then be passed to a genuine site having entered their personal information on the bogus site.

The 'from' box on an email is easily changed to hide the true identity of the sender and should not be relied upon

Don't be fooled by the quality of the web site. There are thousands of good quality web sites set up by criminals for all sorts of activity in addition to obtaining personal details. Many falsely show logos of credit cards, other companies and unauthorised links to genuine web sites

Additional Card Security.

Set up your Credit and Debit cards with 'Verified by Visa' or 'MasterCard SecureCode' when you receive them.

This provides an additional level of security if your card or details are lost or stolen. Even if you do not intend to use the Internet for card transactions,

This is done via your card issuer.

9). Money Transfer Agencies:

Know who you are sending money to.

Money Transfer companies such as Western Union and MoneyGram exist for the transfer of money to somebody that you know. Fraudsters abuse the system by persuading victims to send money to them. People who you do not know!

The Sterling Prevention Team have produced a video showing five different frauds that were perpetrated against people who then used Money Transfer agents to send their money.

- Goods not received – A computer technician paid for pop concert tickets that were advertised in an on-line auction site. They were never received.
- Criminal Cashback – A motor racing mechanic selling a car sent money to a shipping agent after receiving an overpayment cheque, which 'cleared' but was later found to be fraudulent. http://www.met.police.uk/fraudalert/section/cashback_fraud.htm
- Second Chance Offer. – An insurance clerk bid for furniture on an on-line auction site. He did not submit the winning bid but received an offer for the sale of the same furniture from what he thought to be the genuine seller, backed up by a web site. No goods received.
- http://www.met.police.uk/fraudalert/internet_auction.htm
- Honey Trap – A user of a dating site duped to send money to a person involved in a road accident in Nigeria.
- Lottery winner. An elderly widow sent her life savings as a result of being told she had won the Australian Lottery. Her savings included compensation for her husband being killed in a Road Traffic Accident. She also took out a loan when her savings were exhausted and sent this to the fraudsters.
- http://www.met.police.uk/fraudalert/section/lotto_fraud.htm

Operation Sterling continues to work with Money Transfer companies.

http://www.met.police.uk/fraudalert/money_transfer.htm

10) Vehicle Buying, Shipping and Escrow frauds.

The Vehicle Safe Trading Advisory Group (VSTAG) was set up by the Sterling Prevention Unit as the result of the Metropolitan Police having a significant number of fraud allegations reported to them by people buying and selling cars.

These frauds, when successful, can involve several thousand pounds. They vary from simple non delivery frauds, cheque overpayment or cash back frauds to sophisticated shipping and escrow frauds involving fake web sites.

VSTAG members are working to prevent fraudulent adverts being placed on their web sites and block adverts believed to be fraudulent.

ESCROW companies hold payments for goods in safe keeping until the goods have been delivered and the buyer has confirmed safe receipt. This solves many of the problems in handling money during the buying and selling process.

There is a large number of bogus escrow web sites set up by fraudsters to induce victims to send money to accounts controlled by the fraudsters. Any offer to ship a vehicle or pay through an escrow web site should be treated with suspicion.

Payment advice is included in the VSTAG guide.

www.met.police.uk/fraudalert/docs/vstag_adviceguide.pdf

The Office of Fair Trading (OFT).

The Office of Fair Trading (OFT) carried out research in 2006 and estimated that 3.2 million adults in the UK (around 1 in 15 people) collectively lose around £3.5 billion to mass marketing scams each year. This equates to about £70 per annum for each adult living in the UK. Furthermore, half the adult population is likely to have been targeted by a fraud.

11) Allegations of Crime, Complaints and other reports.

The police are not the only agency that have powers to investigate fraud related offences.

If you are unsure whether you are a victim of fraud there are many sources of advice to help you understand what may have happened.

This document and the web sites listed will assist.

What to do if you become a victim of fraud.

If you believe that you are a victim of a criminal offence of fraud, you will need to attend or telephone your local police station to make a report.

Special arrangements apply to the fraudulent use of credit cards, bank debit cards, cheques and bank accounts

- New rules came into affect on 1st April 2007. If your credit card, bank debit card, cheques or account details have been used *fraudulently*, your bank or financial Institution *must* be informed. They have the responsibility to report the fraudulent activity to police.
- If your bank or financial institution will not reimburse you, or your bank has requested you to, a report must be made to the police.

Trading Standards and Consumer issues.

If you have a dispute or complaint about something that you have bought in a shop, by mail order or via the internet, or want some consumer advice, contact Consumer Direct on 08454 040506 or visit their web site www.consumerdirect.gov.uk

Consumer Direct will forward the complaint to the relevant Trading Standards office.

e-Mails and Web Sites.

If you are the victim of fraud, a report should be made, as described above.

Send all banking related 'phishing' emails to: reports@banksafeonline.org.uk

Paypal or eBay related issues should be sent to spooof@paypal.co.uk and spooof@ebay.co.uk respectively.

If you are forwarding emails to the above sites that you believe are fraudulent, please include the email headers. See the Metropolitan Police 'Fraud Alert' web pages about 'Internet headers' for how to do this.

Vehicle Buying and Selling Related frauds.

If the vehicle that you have bought is defective, this is usually a matter for your local Trading Standards Department, make a report via Consumer Direct.

If you find out that the vehicle that you have bought is a stolen vehicle then this is a matter for the police.

If you are the victim of fraud, a report should be made to your local police. More information on what you should do to report a crime in these circumstances is contained in the 'VSTAG' advice document 'Reporting Fraud to Police'.

Operation Sterling

Sterling is the Metropolitan Police initiative to tackle Economic Crime throughout London. By working together with individuals and organisations, from all levels of the private and public sectors, Sterling aims to make London safer from all types of Economic Crime. Innovative new techniques are being developed to prevent, disrupt, and prosecute fraud related offences.

Prevention Toolkit – Sources of Information:

General Information:

Metropolitan Police 'Fraud Alert' Web Site:
www.met.police.uk/fraudalert

Metropolitan Police 'Sterling' Report:
www.met.police.uk/fraudalert/docs/sterling_2005_2008.pdf

Home Office – www.homeoffice.gov.uk

Home Office Crime Reduction Web site:
www.crimereduction.homeoffice.gov.uk

Identity Fraud:

National Identity Fraud Prevention Week
www.stop-idfraud.co.uk

CIFAS Protective Registration:
www.cifas.org.uk/protective_registration.asp

Home Office Identity Fraud Web Site:
www.identitytheft.org.uk/

All Party Parliamentary Group on Identity Fraud:
www.idfraud.org.uk

Secure disposal:

British Security Industries Association:
www.bsia.co.uk/MRXU5X91411_p;LY8M9N53879

Credit Reference Agencies:

Callcredit Plc 08700 60 14 14
www.callcredit.co.uk

Equifax Ltd 08700 100 583
www.equifax.co.uk

Experian Ltd 08702 416 212
www.experian.co.uk

Company Identity Fraud:

Companies House:
www.companieshouse.gov.uk

Monitor, Web Filing and Proof:
www.companieshouse.gov.uk/infoAndGuide/coldFraud.shtml

Payments and Banking:

APACS - the UK payments association:
020 7711 6200 www.apacs.org.uk

Bank Safe Online.
www.banksafeonline.org.uk

CardWatch
www.cardwatch.org.uk

CIFAS:
www.cifas.org.uk/

Financial Services Authority:
www.fsa.gov.uk

Money Transfer Agents:
www.met.police.uk/fraudalert/money_transfer.htm

Criminal Cash Back Fraud:
www.met.police.uk/fraudalert/section/cash_back_fraud.htm

Secure on-line card transactions:
Contact your card issuer.

Shipping and Escrow Payments.

Shipping and Escrow Fraud Information.
www.escrowpolice.org

Shipping and Escrow Fraud Sites.
www.escrow-fraud.com

Vehicle buying and selling:

Vehicle Safe Trading Advisory Group:
www.vstag.org.uk

Metropolitan Police Fraud Alert:
www.met.police.uk/fraudalert

Information for Innocent Purchasers of stolen vehicles:
www.cma.uk.com

Fraud and the Fraud Review:

The Fraud Advisory Panel:
www.fraudadvisorypanel.org

National Fraud Strategic Authority (NFSA)
www.attorneygeneral.gov.uk/national_fraud_strategic_authority_page.html

Scams:

Office of Fair Trading (OFT):
www.oft.gov.uk/

Scambusters:
www.oft.gov.uk/Consumer/Scams/default.htm

On Line Scam Report:
www.oft.gov.uk/oft_at_work/consumer_initiatives/scams/

Scams Leaflets these are available to be printed as PDF documents, ordered on-line or by phoning 0800 389 3158:

Recommended leaflets:

- How to recognise a scam
- Scambuster
- Can you stop the person you care for being scammed?

www.oft.gov.uk/advice_and_resources/publications/consumer_advice/scams/

Cronic Scam Victims Support and Advice:
www.thinkjessica.com

Preference Services

Avoiding revenue generating phone numbers:
www.saynoto0870.co.uk

Telephone Preference Service:
0800 398893.
www.tpsonline.org.uk.

Fax preference service:
020 7291 3330
www.tpsonline.org.uk/fps/

Mail Preference Service: 0207 2913300
www.mpsonline.org.uk

Royal Mail opt out: 08457 950 950
eMail optout@royalmail.co.uk

Phone Pay Plus (formerly ICSTIS):
www.phonepayplus.org.uk

OFCOMM web site:
www.ofcom.org.uk/consumeradvice

Intellectual Property and Copyright:

The Intellectual Property Office (Formerly the Patent Office). www.ipo.gov.uk

Federation Against Copyright Theft: - Film Piracy: 020 8568 6646.
www.fact-uk.org.uk

BPI (British Phonographic Industry) – Music www.bpi.co.uk

Vulnerable and elderly people:

Public Guardianship Office (PGO):
0845 330 2900 www.guardianship.gov.uk

PGO Guide 'Who we are and what we do':
<http://www.publicguardian.gov.uk/docs/OPG502-1007.pdf>

Forms & booklets by phone or download;
www.publicguardian.gov.uk/forms/forms.htm

British Bankers Association guide for people who lack capacity.
<http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=138&a=10884>

Data Protection: ICO guides:
www.ico.gov.uk

Action on Elder Abuse:
www.elderabuse.org.uk

Help the Aged:
www.helptheaged.org.uk

Leaflets:
<http://www.ageconcern.org.uk/AgeConcern/InformationOrderForm.asp>

Age Concern:
www.ageconcern.org.uk

Internet and eMail.

Get Safe On Line
www.getsafeonline.org

Bank Safe On Line:
www.banksafeonline.org.uk

Internet headers:
www.met.police.uk/fraudalert/internet_headers.htm

Send bank related 'phishing' emails to:
reports@banksafeonline.org.uk

Send Paypal or eBay related issues to:
spoofer@paypal.co.uk or spoofer@ebay.co.uk