

# Metropolitan Police - Operation Sterling:

## Personal Prevention Toolkit

***"An ounce of prevention is better than a pound of cure"***  
*Judge Henry DeBracton, c1240.*

**This document aims to provide a range of practical advice to reduce vulnerability to fraud, and other financial issues.**

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.

A 'scam' is usually viewed as low in value, but there may be a high number of offences. 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.

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

Under the Fraud Act 2006, fraud is committed in three ways: False representation, Failing to disclose information, and Abuse of position. There are many other specific fraud offences.

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.

Other Sterling activities include participation in the National Identity Fraud Prevention Week and the 'Silence of the Scams' campaign to combat mass marketing fraud.

### **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. The Internet and e-Mail.
3. Mass Marketing Fraud.
4. Doorstep Crime and Bogus Callers.
5. Phone Calls and Call Costs.
6. Marketing phone calls and Junk mail.
7. Vulnerable Groups and Financial Abuse.
8. Managing Money - Banks and Cards.
9. Money Transfer
10. Vehicle Buying and Selling, Shipping and Escrow fraud.
11. House and property purchase and take-over fraud.
12. Reporting Fraud

Appendix: Sources of Information and Links.

### **Operation ST£RLING**

**The Metropolitan Police initiative to tackle Economic Crime throughout London.**



## 1) Identity Fraud.

Identity Fraud has become a major issue and concern to all. Many frauds involve the unauthorised use of other peoples information taken from 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 misusing their personal details.

Callcredit Plc 08700 60 14 14  
[www.callcredit.co.uk](http://www.callcredit.co.uk)

Equifax Ltd 0800 121 4752  
[www.equifax.co.uk](http://www.equifax.co.uk)

Experian Ltd 0844 481 8000  
[www.experian.co.uk](http://www.experian.co.uk)

The Credit Reference Agencies offer free advice to victims of Identity Fraud.

[www.identitytheft.org.uk/victims-of-fraud-service.asp](http://www.identitytheft.org.uk/victims-of-fraud-service.asp)

**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: 0330 1000 180 (local rate) or e-mail:  
[protective.registration@cifas.org.uk](mailto:protective.registration@cifas.org.uk)

## 2) 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](http://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. New threats 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.

Never reply to a bogus email or click on a link in one.

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

### 3) 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, get-rich quick schemes, clairvoyants, fake health cures, bogus sweepstakes and lotteries, are some of the favoured means of separating the unwary from their money. The number and variety of scams keeps on growing.

More information from the Citizens Advice consumer service on 08454 040506 or [www.adviceguide.org.uk](http://www.adviceguide.org.uk)

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

[www.offt.gov.uk/OFTwork/publications/publication-categories/consumer\\_advice](http://www.offt.gov.uk/OFTwork/publications/publication-categories/consumer_advice)

**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.

**You are not the only person that they will be trying to con!**

#### **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.

#### 4) 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 roof or building 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 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 any 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.**

**The Metropolitan Police  
non-urgent call number is now**

**101**

#### 5) Phone Calls and Call Costs.

Unwanted phone calls can be much more than a nuisance and 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](http://www.saynoto0870.co.uk).

Further information can be found at the Phone Pay Plus and OFCOM web sites

[www.phonepayplus.org.uk](http://www.phonepayplus.org.uk)

<http://consumers.ofcom.org.uk>

## 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 has 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'. The call will be a competition, survey or offer but it could 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](http://www.tpsonline.org.uk)

The fax preference service is on 020 7291 3330 or at [www.tpsonline.org.uk/fps/](http://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](mailto:optout@royalmail.com) or telephoning 08457 950 950.

**Register your Phone, Laptop and other gadgets and valuables with [www.immobilise.com](http://www.immobilise.com)**

## 7) Vulnerable Groups and Financial Abuse.

Those less able to look after themselves can often be subject to financial exploitation.

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.

Many people require help in managing their day-to-day activities – talking on the phone, understanding letters and correspondence.

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. 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.

Organisations must ensure that their data is accurate and up to date, and individuals have a right to prevent processing. If somebody wants an elderly relative removed from a mailing list the record must be updated.

DWP and the Post Office Card Accounts can allow another person to receive payment.

Banks may allow customers to sign a 'Third Party Mandate' allowing others to operate any account on behalf of a relative or a person they care for. This may restrict the person to branch use only and not allow a carer to view or use the accounts on line.

Another option is to become a joint account holder which makes both people jointly liable for the account and has other implications. See the BBA guide for more information.

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.

### Carers

See our links page for organisations that support you - you too are important.

## 8) Managing Money - Banks and Cards.

Looking after money is becoming increasingly complex, with new ways of managing money and organisations promoting internet banking in preference to face to face services. Many people still do not have a bank account or access to the Internet. This is a matter of choice, and many people may not be able to use computers or even make phone calls.

Older and vulnerable people are particularly affected by this and may have always used cash to manage their money. There may be a point at which people can no longer continue making payments in person and bills would be better managed using bank accounts.

One issue is the amount of marketing from organisations, including banks. Opt out where you can, follow the advice in our section on marketing phone calls and junk mail. See also the previous section on vulnerable groups.

Payments from the Department of Work and Pensions (DWP) which include benefits and pensions may be paid into Bank Accounts, into a Post Office Card Account or in exceptional circumstances via a giro cheque.

The Bank account may be a normal 'Current' account operated by all banks and most building societies. 'Basic' bank accounts have limited services and are suitable for those who not had a bank account before.

The Post Office Card Account (POCA) was established to replace cheques issued by the DWP. This does not operate as a normal bank account as there is no interest paid or facilities to pay bills or transfer money. Money can only be withdrawn in Post Offices or using Post Office ATM's (Cash Machines).

DWP payments can be paid into a Bank Account, which has the benefit of allowing payments to be made electronically.

- Banks Accounts which issue 'Debit' cards usually allow money to be withdrawn at ATM's (Cash Tills), so you are not restricted to bank branches.
- Most banks allow money to be withdrawn at post offices from basic bank accounts, some from current accounts.

Details of Post Office facilities for Bank Account holders can be found on their web site [www.postoffice.co.uk](http://www.postoffice.co.uk) under "Counter Money Services" or from a post office.

## Chip and Signature cards:

Issuers of debit and credit cards must give an alternative to 'Chip and PIN' cards to people who are unable to remember a PIN or use a PIN machine.

- If you have trouble remembering your PIN or in using keypads, contact your bank to get a chip and signature card instead.
- 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, a receipt is printed for the assistant to give you to sign.
- All the retailer needs to do is to follow the instructions on their 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 CHIP cards without a PIN.
- In some supermarkets you now have to ask for "cash back", which is helpful if you have a chip and signature card.
- Some banks allow use of a 'CHIP and Signature' card in their cash machines. Users still have to input their PIN. This is helpful to people who cannot use small shop machines but can still use cash tills.
- Most banks allow money to be withdrawn at post offices from basic bank accounts, some from current accounts, using a PIN.
- A 'Chip and Signature' card is not available with the Post Office Card Account issued to Benefit and Pension recipients due to DWP Rules.

## 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, protect yourself using this facility. Your card issuer may have their own name for this service, which is also known as '3D Secure'.

## 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 and trust. 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. [www.met.police.uk/fraudalert/cashback\\_fraud.htm](http://www.met.police.uk/fraudalert/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. [www.met.police.uk/fraudalert/internet\\_advertising\\_auction.htm](http://www.met.police.uk/fraudalert/internet_advertising_auction.htm)
- Honey Trap – A user of a dating site duped to send money to a person involved in a road accident in Nigeria. [www.met.police.uk/fraudalert/money\\_transfer.htm](http://www.met.police.uk/fraudalert/money_transfer.htm)
- 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. [www.met.police.uk/fraudalert/mass\\_market\\_fraud.htm](http://www.met.police.uk/fraudalert/mass_market_fraud.htm)

### Money Transfer is the favourite way for fraudsters to receive money from you.

- [www.met.police.uk/fraudalert/money\\_transfer.htm](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.

Buying and selling advice is included in the guide:

[www.met.police.uk/fraudalert/buying\\_selling\\_vehicles.htm](http://www.met.police.uk/fraudalert/buying_selling_vehicles.htm)

If a vehicle that you have bought is defective, and the problem is not resolved, this is usually a matter for advice from your local Trading Standards Department, who are contacted 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 'Action Fraud' as detailed in this document. More information on reporting a crime in these circumstances is contained in the 'VSTAG' advice document 'Reporting Fraud to Police'.

[www.vstag.co.uk](http://www.vstag.co.uk)

## 11) House and property purchase and take-over fraud.

Exaggerating income or making false statements to borrow more money is Fraud.

- Don't be tempted to provide fake paperwork, such as payslips, or false references.
- Beware of complicit professionals who support exaggerated applications.
- Exaggerated property valuations and 'cash back schemes may be illegal.
- Other mortgage frauds may implicate the unwary in criminal networks.

### Property Takeover Fraud.

Taking over a property by fraudulently changing the property deeds/title is now common. This often happens when the property is owned outright and the property is rented out, or by squatters. The owner's identity is assumed to carry out the fraud.

### Protection and Prevention Measures.

If you are a house owner your name is listed at the Land Registry as the owner of the property. Your mortgage company will have a charge on your property.

- Title deeds have been replaced by automated systems for conveyancing.
- Property owners can add additional addresses for any letters from the Land Registry. Changes to records can be notified to solicitors or to your home address if you have a rental property.
- Carers for vulnerable people, especially the elderly can also nominate other persons and addresses for notification of changes to Land Registry records.
- There is a significant amount of land in the UK that is unregistered. The Land Registry provides advice about registering and purchasing unregistered land.

The following Land Registry guides are recommended. [www.landregistry.gov.uk](http://www.landregistry.gov.uk)

- How to safeguard against property fraud.
- Keeping your address for service up to date

Note that there are other sites offering advice and access to the land registry documents. These sites may charge a premium, as much as £10 more for a document download that is available from the official government site.

## 12) Allegations of Crime, Complaints and other reports.

### In an emergency you should phone 999

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

### What to do if you become a victim of fraud.

If you believe that you are a victim of a criminal offence of Fraud, often also referred to as 'scams', you should make a report.

The National Fraud Reporting Centre "Action Fraud" is available to report fraud offences on line or by phone. [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

Local Police should take a formal report of fraud in the following circumstances:

1. Where the person suspected of committing the crime can be easily identified.
2. Where the person reporting or the victim is vulnerable. A 'third party' can report fraud.
3. Where the crime is in progress.

### Cards, Cheques and Bank Accounts.

Special arrangements apply to the fraudulent use of Credit Cards, Bank Debit Cards, Cheques and Bank Accounts.

If your credit card, bank debit card, cheques or account details have been used fraudulently, your bank or financial Institution must be informed. They make a formal report.

If your bank or financial institution will not reimburse you, or your bank has requested you to, make a report to Action Fraud.

### 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 the Citizens Advice consumer service on 08454 040506 or visit their web site [www.adviceguide.org.uk](http://www.adviceguide.org.uk)

Citizens Advice will forward the complaint to the relevant Trading Standards office.

**ActionFraud**  
Report Fraud & Internet Crime  
**0300 123 2040**  
[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

## Prevention Toolkit - Sources of Information and Links:

### General Information:

Metropolitan Police 'Fraud Alert' Web Site:  
[www.met.police.uk/fraudalert](http://www.met.police.uk/fraudalert)

Home Office – [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk)

Home Office Crime Reduction Web site:  
[www.homeoffice.gov.uk/crime](http://www.homeoffice.gov.uk/crime)

### Identity Fraud:

National Identity Fraud Prevention Week  
[www.stop-idfraud.co.uk](http://www.stop-idfraud.co.uk)

CIFAS Protective Registration:  
[www.cifas.org.uk/protective\\_registration.asp](http://www.cifas.org.uk/protective_registration.asp)

Identity Fraud Communications Awareness Group (IFCAG) [www.identitytheft.org.uk/](http://www.identitytheft.org.uk/)

### Secure disposal:

British Security Industries Association:  
[www.bsia.co.uk/MRXU5X91411\\_p;LY8M9N53879](http://www.bsia.co.uk/MRXU5X91411_p;LY8M9N53879)

### Credit Reference Agencies:

Callcredit Plc 08700 60 14 14  
[www.callcredit.co.uk](http://www.callcredit.co.uk)

Equifax Ltd 08700 100 583  
[www.equifax.co.uk](http://www.equifax.co.uk)

Experian Ltd 08702 416 212  
[www.experian.co.uk](http://www.experian.co.uk)

### Company Credit Reference Agencies

Dun & Bradstreet  
[www.dnb.com/uk](http://www.dnb.com/uk)

### Company Identity Fraud:

Companies House:  
[www.companieshouse.gov.uk](http://www.companieshouse.gov.uk)

Monitor, Web Filing and Proof:  
[www.companieshouse.gov.uk/infoAndGuide/colDFraud.shtml](http://www.companieshouse.gov.uk/infoAndGuide/colDFraud.shtml)

### Reporting Fraud.

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)  
0300 123 2040 (local call rate).

### Payments and Banking:

Money Advice Service (Govt Advice):  
[www.moneyadviceservice.org.uk](http://www.moneyadviceservice.org.uk)

Types of Bank Account.  
[www.direct.gov.uk/en/MoneyTaxAndBenefits/ManagingMoney/index.htm](http://www.direct.gov.uk/en/MoneyTaxAndBenefits/ManagingMoney/index.htm)

UK payments. [www.ukpayments.org.uk](http://www.ukpayments.org.uk)

Payments Council  
[www.paymentscouncil.org.uk](http://www.paymentscouncil.org.uk)

Bank Safe Online. [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)

British Bankers Association. [www.bba.org.uk](http://www.bba.org.uk)

Financial Services Authority: [www.fsa.gov.uk](http://www.fsa.gov.uk)

**Money Transfer Agents:**  
[www.met.police.uk/fraudalert/money\\_transfer.htm](http://www.met.police.uk/fraudalert/money_transfer.htm)

Cards for disabled customers.  
[www.theukcardsassociation.org.uk/individual/cards-disability-issues.asp](http://www.theukcardsassociation.org.uk/individual/cards-disability-issues.asp)

### Shipping and Escrow Payments:

Shipping and Escrow Fraud Sites.  
[www.escrow-fraud.com](http://www.escrow-fraud.com)

### International Complaints:

Econsumer.gov. [www.econsumer.gov/english](http://www.econsumer.gov/english)

### Vehicle buying and selling:

Vehicle Safe Trading Advisory Group:  
[www.vstag.co.uk](http://www.vstag.co.uk)

Metropolitan Police Fraud Alert:  
[www.met.police.uk/fraudalert](http://www.met.police.uk/fraudalert)

**Insurance Fraud Bureau:**  
[www.insurancefraudbureau.org](http://www.insurancefraudbureau.org)

### Fraud and the Fraud Review:

The Fraud Advisory Panel:  
[www.fraudadvisorypanel.org](http://www.fraudadvisorypanel.org)

National Fraud Authority (NFA):  
[www.homeoffice.gov.uk/agencies-public-bodies/nfa/](http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/)

## Scams:

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

Scambusters:  
[www.oft.gov.uk/Consumer/Scams/default.htm](http://www.oft.gov.uk/Consumer/Scams/default.htm)

Scams Leaflets these are available as PDF docs, 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](http://www.oft.gov.uk/advice_and_resources/publications/consumer_advice/scams)

Safe From Scams  
[www.safefromscams.co.uk](http://www.safefromscams.co.uk)

Chronic Scam Victims Support and Advice:  
[www.thinkjessica.com](http://www.thinkjessica.com)

Romance Scams and Honeytraps  
[www.romancescam.com](http://www.romancescam.com)

## Preference Services

Avoiding revenue generating phone numbers:  
[www.saynoto0870.co.uk](http://www.saynoto0870.co.uk)

Telephone Preference Service:  
0800 398893. [www.tpsonline.org.uk](http://www.tpsonline.org.uk).

Fax preference service:  
020 7291 3330 [www.tpsonline.org.uk/fps](http://www.tpsonline.org.uk/fps)

Mail Preference Service: 0207 2913300  
[www.mpsonline.org.uk](http://www.mpsonline.org.uk)

Royal Mail opt out: 08457 950 950  
eMail [optout@royalmail.co.uk](mailto:optout@royalmail.co.uk)

Phone Pay Plus: [www.phonepayplus.org.uk](http://www.phonepayplus.org.uk)

OFCOMM web site:  
<http://consumers.ofcom.org.uk>

## Intellectual Property and Copyright:

The Intellectual Property Office (Formerly the Patent Office).  
[www.ipo.gov.uk](http://www.ipo.gov.uk)

Federation Against Copyright Theft: - Film Piracy: 020 8568 6646. [www.fact-uk.org.uk](http://www.fact-uk.org.uk)

BPI (British Phonographic Industry) – Music  
[www.bpi.co.uk](http://www.bpi.co.uk)

## Vulnerable and elderly people:

Action on Elder Abuse [www.elderabuse.org.uk](http://www.elderabuse.org.uk)

AgeUK the new name for Help the Aged and Age Concern: [www.ageuk.org.uk](http://www.ageuk.org.uk)

Leaflets: [www.ageuk.org.uk/publications](http://www.ageuk.org.uk/publications)

Alzheimer's Society [www.alzheimers.org.uk](http://www.alzheimers.org.uk)

Dementia UK: [www.dementiauk.org](http://www.dementiauk.org)

Friends of the Elderly [www.fote.org.uk](http://www.fote.org.uk)

Office of the Public Guardian (OPG):  
0845 330 2900  
<http://www.direct.gov.uk/en/Governmentcitizensandrights/Mentalcapacityandthelaw/index.htm>

Forms & booklets by phone or download;  
[www.justice.gov.uk/global/forms/opg/index.htm](http://www.justice.gov.uk/global/forms/opg/index.htm)

British Bankers Association guides:  
[www.bba.org.uk/publications](http://www.bba.org.uk/publications)

Information Commissioners Office:  
[www.ico.gov.uk](http://www.ico.gov.uk)

## Carers

Carers UK: [www.carersuk.org](http://www.carersuk.org)

Crossroads caring for carers:  
[www.crossroads.org.uk](http://www.crossroads.org.uk)

The Princess Royal trust for Carers:  
[www.carers.org](http://www.carers.org)

## Land Registry

Land Registry [www.landregistry.gov.uk](http://www.landregistry.gov.uk)

## Internet and eMail.

Get Safe On Line [www.getsafeonline.org](http://www.getsafeonline.org)

Bank Safe OnLine [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)

Send bank related 'phishing' emails to:  
[reports@banksafeonline.org.uk](mailto:reports@banksafeonline.org.uk)

Send Paypal or eBay related issues to:  
[spoof@paypal.co.uk](mailto:spoof@paypal.co.uk) or [spoof@ebay.co.uk](mailto:spoof@ebay.co.uk)

Other scam emails should be forwarded to:  
[email@actionfraud.org.uk](mailto:email@actionfraud.org.uk)