Another Legal Guide from Bonallack & Bishop Solicitors

80 PRACTICAL TIPS

TO HELP COMBAT

ALL YOU NEED TO KNOW

BONALLACK & BISHOP
SOLICITORS

Over the last few years, identity theft has become one of the fastest growing crimes in the UK.

With practices varying from the most technical of internet hacks to trawling through rubbish bins looking for pieces of your personal information – it's not surprising that identity theft problems are hard to prosecute and can often be hard to understand.

We are providing this booklet to help you help yourself. If you become a victim of identity theft and feel that you need some legal advice, then please do not hesitate to contact us.

What is identity theft?

Identity theft is the term used when your personal information is used by someone else without your knowledge, often fraudulently in connection with a criminal activity. Some of the most common forms of identity theft in the UK include:

- fraudulent use of a credit card or applying for a new credit card
- using mobile phone or utility accounts fraudulently
- opening new bank accounts

The Government estimates that over 100,000 people in the UK are affected by identity theft each year and this is costing the UK economy in the region of £1.3 billion. This booklet outlines various tips to help prevent someone getting hold of your identity and using it.

BONALLACK & BISHOP
SOLICITORS

Rougemont House
Rougemont Close
Manor Road
Salisbury
SP1 1LY

Tel: 01722 422300
Fax: 01722 422121
Email: Salisbury@bishopslaw.com
www.bishopslaw.co.uk

SECTION 1: GENERAL TIPS

1. Report any lost or stolen documents that contain personal information (e.g. passport, driving licence, bank cards) immediately to the company that issued them.

2. If you're thinking of selling your computer be sure to erase all its data using proprietary software first. You might be surprised to know that identity thieves scour the papers and internet looking for second hand computers.

3. Make sure that your signature is not easy to forge.

4. Check your credit report – this can be done completely free online or a paper copy can cost as little as £2 and is well worth the peace of mind. The report provides credit history as well as any fraud attempts which have been made against your name. Contact *Callcredit, Equifax* or *Experian*,(which also provides a monitoring service at £6.99/month), or obtain online credit files from **www.checkmyfile.com** or **www.annualcreditreport.co.uk**

5. If you have been, or think you are likely to become, the victim of identity theft, register yourself with an identity monitoring service to get independent expert advice.

6. In a restaurant, don't part with your card before you've received your order. If the establishment needs to hold your card for security/tab, be sure that it's given to the right person and that it's held securely.

7. Always keep your cheque book separate from your cheque guarantee cards.

8. Don't keep your home address attached to your keys or anywhere in your wallet.

9. Don't carry your driving licence around with you – you rarely need it. If you ever get stopped in a motor vehicle by the police, they will give you sufficient time to produce your documentation.

SECTION 2: THE INTERNET

10. Make sure you have up-to-date anti virus software on your computer.

11. Make sure you have a firewall installed. It's a barrier put up on your computer to prevent hackers getting access.

12. Scan your computer for spyware with a tool such as Ad-Aware.

13. When purchasing anything over the Internet make sure you can see the padlock symbol at the bottom of the page and that the standard 'http://' in your address bar has changed to 'https://' which indicates that the page is secure.

14. With any high-value transactions being received over the internet, it's a good idea to make sure you receive the payment first before you dispatch any goods or services.

15 Use Escrow accounts for online payments where the release of funding is subject to the fulfilment of certain requirements.

16 Check your account transactions and statements online at least once per week, and look out for anything which looks suspicious. If you do see something, report it to your bank immediately.

17 Avoid using wireless networks in public places as they do not provide a secure connection and can be easily hacked. Identity thieves sometimes also use small transmitter devices to set up their own wireless network in a public place – if someone connects, any personal information stored on the laptop can be extracted.

18 Providing personal information which is put on public display on social networking sites can be risky. Weigh up the risks before submitting any personal details to sites such as Facebook or MySpace.

19 Always be sure to log out of any web account before you leave your PC. This deters anyone (either in work or in a public place) from just opening up a browser and viewing cached pages (stored copies of the pages you have recently viewed on your PC) to gather personal information.

SECTION 3: EMAIL

20 Banks shouldn't contact you via email, asking you to 'activate your account'. If you get one of these messages, it's most likely a fraudster trying to steal your details. This is what is known as "phishing". If you do get one of these emails, click <Shift><Delete> without opening it.

21 If you're in any doubt about the authenticity of the sender of any emails you receive, get in contact directly with the company in question.

22 If you speak to anyone from your bank on the phone – be sure to ask them to verify their identity too! Your bank will normally ask you to verify who you are from recent transactions / standing orders / Direct Debits on your own account.

23 Don't email personal or sensitive information/ bank details.

SECTION 4: POSTAL MAIL

24 Make sure that your mail is delivered to you securely – if you have a shared lobby or an external mailbox you are at a greater risk of your mail being intercepted.

25 Opt for paperless bank statements if possible – this generally offers more protection than receiving paper statements (and is more environmentally friendly!). However, if you do receive paper statements, make sure the bank has your current address.

26 Get in touch with Royal Mail if you think you are missing any mail.

27 Use "Signed For" if sending any sensitive or valuable information.

28 If you are moving house, get your mail redirected, do not rely on collecting it from the people at your old address.

29 Deposit your mail securely in a post box / post office rather than leaving it in a mail out-tray at work.

SECTION 5: BANK CARDS

30 Report lost or stolen bank cards immediately. The most common type of card fraud is where a criminal has obtained your cards and poses as you to obtain goods or services – and this all normally happens before you even notice your card has gone missing!

31 Credit cards are generally more secure than debit cards, as transactions can be reviewed before the money leaves your account.

32 Credit card skimming is another common type of card fraud and involves a card going through a device (without your knowledge) that copies the data from your card's magnetic strip electronically. This data can then be transferred to another card for use. Try and use cash machines which are inside your bank as these are less likely to have been tampered with using a skimming device. Franchised petrol stations have been widely reported for 'skimming' credit cards.

33 CNP (Card not present) Fraud is now the largest type of credit card fraud in the UK and the main problem here is that neither the card holder nor the actual card are present during the transaction (i.e. payments taken over the phone). In these cases, businesses are unable to check the security features of the card to see if it's genuine and can't check whether the customer is actually the cardholder. Even the card issuer can't confirm that the information provided in the transaction has been given by the genuine cardholder! To avoid fraudulent CNP transactions always be wary when using your credit/ debit card over the phone as you never know who may be listening and recording this information.

34 If you ever have to write your card details down on paper, ensure that the paper is disposed of securely.

35 Make sure you sign your card as soon as you get it. A lot of places will still accept signatures rather than chip-and-pin.

36 Keep your eye on the expiry date of your debit/credit cards as your bank should issue you with a new card before the date has expired. If you haven't received anything contact them immediately.

37 If you are due to receive a new card/cheque book from your bank, arrange to collect it directly from your branch if possible rather than have it posted to you.

38 Write a random 4-digit number on the back of your credit and debit cards. This way, if your card is stolen (assuming the thief hasn't used skimming or camera devices) then there's a possibility the thief will try the random code 3 times and block your PIN.

SECTION 6: PASSWORDS/ PINs

39 Keep the contact numbers for all your bank accounts somewhere handy in case your wallet/purse/handbag is stolen or lost, this way you can cancel all your cards immediately. If you are moving house, get your mail redirected, do not rely on collecting it from the people at your old address.

SECTION 7: TELEPHONE

40 Create passwords / PINs which aren't easy to guess.

41 Never write your PIN down – always memorise it.

42 Do not use the same PINs / passwords for different accounts.

43 Update passwords regularly.

44 For computer passwords – use a mixture of upper and lower case and include numbers.

SECTION 8: AT WORK

45 Avoid giving out personal information on the phone.

46 Be aware of your surroundings if talking in a public place (eg. don't phone your bank while sitting on the train!).

47 Get your home number listed as ex-directory.

48 If you receive a phone call (often automatic) informing you that you have won a prize, this could well be a fraudster trying to obtain personal details.

49 TPS (Telephone Preference Service) – avoid unwanted marketing and sales calls which could possibly be fraudulent, by registering your telephone number with the Telephone Preference Service.

EMPLOYEES:

50 Change your computer passwords regularly.

51 Do not use Post-Its stuck to your computer to remember your passwords.

52 If you're concerned about the security on your PC talk to your IT manager- don't install your own protection software as this could compromise the network.

EMPLOYERS:

53 Corporate identity theft is when a company's identity is used fraudulently in order to obtain credit, goods or services. This can have a detrimental effect on the reputation and the credit record of the company, and can ultimately lead to bankruptcy. Make sure your staff are well informed of the risks of corporate identity fraud, keeping everyone up to date will ensure they are more vigilant.

54 Ensure that your staff verify who they are speaking to before divulging company information over the phone. Take a number and call someone back if you are unsure who they are.

55 Make sure that you keep company bank account information secure.

56 Keep all of the computers password protected and make sure that these are updated regularly.

57 Keep the building secure, make sure you know who has keys and use the type of key that are hard to duplicate.

58 Make sure that the people handling your invoices are aware of the risks of identity theft – and that unusual invoices or payment demands are dealt with immediately. Check invoices and that the goods are actually received – someone can file a form against your company to change the registered address for a short period of time. (Sky Marketing Ltd in Nov 2003 + Staples) – then make huge orders and then file another Form 287 at Companies House to change address back. Similar methods could be used to change names of directors, maybe negotiate bank loans…with only a small risk of detection.

59 Make sure you dispose of your documents securely. If you are a small company, invest in a shredder before recycling your documents.

60 If you are a company director your details will be on public record – including your home address and possibly your signature. Never reveal your place of birth to someone you don't trust very well.

61 Keep your passport, driving licence, birth and marriage certificates safe at all times and don't part with them unless absolutely necessary. Even copies of your birth certificate contain valuable information for identity thieves.

SECTION 9: AT HOME

62 Make sure that any access points to your home are secure when you go to bed, leave the house or even when you're not in that area of your home.

63 Keep any outbuildings and vehicles securely locked and avoid leaving personal information in them.

64 Don't keep your vehicle registration documents in your vehicle.

65 Don't leave a house or window key anywhere outside – if you're worried about losing your keys or getting locked out, ask a friend or trusted neighbour to hold a key for you.

66 Get a security system installed in your home – this doesn't have to be a state of the art piece of equipment - just the fact that you have one visible is often a valid deterrent.

67 Keep important documents secure in a safe.

68 For the less technically minded, going through a rubbish or recycling bin is an easy way to learn about you and collect your personal information. Information that you may not think of as important such as personal letters, utility bills, insurance documents and bank statements all carry valuable information that can be used to steal your identity, so take care when disposing of these.

69 Put your rubbish and recycling bins out as close to collection time as possible to avoid any unwanted snooping.

70 Invest in a shredder for your home. Not only does this ensure your personal information doesn't get into the wrong hands but can also provide great hamster bedding!

SECTION 9: AT HOME

71 Ask a trusted neighbour or family member to check on your house if you go away for any period of time.

72 Get your mail held securely at your local post office if you go away for a long period of time.

73 If you get regular deliveries to your house (e.g. milk/paper) make sure you cancel these before you go away.

74 Whilst away on holiday, only carry the credit cards that you are likely to need.

75 Ensure that any credit/debit cards that you are not taking with you are stored securely.

76 Don't display your home address or home phone number on any of your luggage – leave a work address or a mobile number.

77 Keep your passport and travel document separate from your credit and debit cards.

78 When you check in to your hotel, try and register using your work address and a mobile number rather than any of your home details.

79 The USA and the Middle East are known as 'hotspots' for identity theft. On return from your visit to either these places check your bank and credit card statements.

80 If the hotel has a room safe, use it. If not then ask if there is a central safe you can put documents, money etc in.