



# How to protect yourself from fraud

essential information  
for your own protection

Financial crime is growing fast and everyone is a target. This leaflet explains how you can help us to protect yourself from being a victim of fraud.

## HELP US TO FIGHT FRAUD

### Know who you're dealing with

Never respond to any unprompted phone calls, emails or text messages asking you for personal or financial information - you may be giving a criminal your details.

Cumberland Building Society will not call or email customers for account information such as account number, personal identification number (PIN) or card details.

Should you wish to verify the identity of a person claiming to call from the Cumberland Building Society, staff members are willing to answer any questions of a non-confidential nature to assure you that the call is genuine.

Alternatively you may request the option to call-back to verify that the call originates from the Society. For calls originating from a branch, the number can be verified in the telephone directory.

Meanwhile calls from the Society's Head Office can be returned via our Customer Contact Team on 0845 601 8396, which can also be verified in the telephone directory.

### Look after your chequebooks and cards

- Always keep your chequebook separate from your cards.
- Never leave them unattended, even at work.
- If you're expecting a card or chequebook in the post and it doesn't arrive, contact us to make sure it hasn't been lost or stolen.
- Guard your cards – treat them in the same way that you would treat your cash.
- Don't let them out of your sight when making a transaction.



Whether or not you shop online, in the wrong hands your card details can be used to shop online. To protect your card, please register your Visa debit cards

for Verified by Visa (VbV). This free service provides additional security and password protects your Visa debit card against unauthorised online use. Even if you do not shop online, it is important to protect your card.

If you have internet access, register online at [www.cumberland.co.uk](http://www.cumberland.co.uk) or register whilst shopping at a VbV registered retailer.

Never...

- write down or record your password in a way which could easily be understood by someone else
- choose a password which could be easy for others to guess
- allow anyone else to use your password,
- tell anyone your password (this includes family, friends, members of our own staff (Cumberland Building Society will never ask you for your password) and the Police) - you are the only one that should ever know it!

If you don't have internet access, please phone our Customer Service Helpline to complete registration.

Further information on VbV is available on [www.cumberland.co.uk](http://www.cumberland.co.uk) or can be obtained from any Cumberland branch.

### Never tell anyone your PIN

You must take all reasonable steps to keep your PIN a secret at all times. In particular you must:

- Memorise your PIN and immediately destroy the form we send you notifying you of it.
- Never write down or record your PIN in a way that could easily be understood by someone else.
- Never choose a PIN which would be easy for others to guess.
- Not tell anyone your PIN (this includes family, friends, members of our own staff (Cumberland building Society will never ask you for your PIN) and the Police) - you are the only one that should ever know it!
- Not allow anyone else to use your card and PIN.
- Take care to shield the entry of your PIN to avoid this being seen by others.
- Remember that you can change your PIN at any Cumberland, Link or Visa cash machine.

### Destroy unwanted financial or personal papers

- Always shred documents such as bills, bank statements and receipts before throwing them away. Card details appear on some receipts so keep them safe or dispose of them carefully. If you don't do this, criminals can find out your name, address and other details by going through your household rubbish.

### Check your statements

- Regularly check your statements for unfamiliar transactions.
- Check your receipts against your statements carefully. If you find an unfamiliar transaction, contact us immediately.
- Let us know immediately if you notice anything unusual on your statements.
- If you're expecting a statement in the post and it doesn't arrive, please tell us.

## CASH MACHINE SECURITY

### Use cash machines carefully

Cash machines are a convenient and safe way to withdraw money and get information about your account. However, criminals do target cash machines, so please use this guidance to protect yourself and your money.

### How can you use cash machines safely?

#### Choosing a cash machine

- Avoid, for example, poorly lit machines when it is dark.
- Be aware of others around you. If someone close by the machine is behaving suspiciously or makes you feel uncomfortable use another one.
- If there is anything unusual about the cash machine or there are signs of tampering, do not use the machine and report it to the building society, bank, Police or premises owner immediately.



#### Using a cash machine

- Give other users space to enter their PIN in private. We recommend standing about two metres away from the user in front of you until the person has completed their transaction. Some cash machines may have a 'safety' zone marking out this area on the ground around the machine.
- Be aware of your surroundings, if someone is crowding you or watching you, cancel the transaction and go to another machine.
- Do not accept help from 'well-meaning' strangers and never allow yourself to be distracted.
- Stand close to the cash machine and always shield the keypad with your free hand to avoid anyone seeing you enter your PIN.

#### Leaving a cash machine

- Once you have completed a transaction, discreetly put your money and card away before leaving the cash machine.
- If the cash machine does not return your card, report its loss immediately to your bank or building society.
- Dispose of your cash machine receipt, mini-statement or balance enquiry with care. Tear up, or preferably shred, these items before discarding them.

#### Key messages

- Cash machines are an obvious target for fraudsters, as wherever there is cash potentially there is crime. However, the chances of this happening to you are still thankfully very low and the industry is working hard to keep it this way.
- It is much safer to carry a card around than cash and if you are a victim of card fraud you will not suffer any financial losses unless you have been negligent (for instance if you have written down your PIN or VbV password).

## USING YOUR CARD ABROAD

### Before you go away

- Only take the cards you intend to use – store the rest securely at home.
- Make a note of your card issuers' emergency contact numbers and keep the information somewhere other than your purse or wallet.
- Make sure your card company has up-to-date contact details for you, including a mobile number if possible.
- If your cards are registered with a card protection agency, ensure you have their contact number and your policy number with you.

### When you are away

- Take the same precautions as you would in the UK. Look after your cards and card details, and shield your PIN with your free hand when typing it into a keypad in a shop or at a cash machine.
- Consider wearing a concealed money belt to keep your cards, cash and traveller's cheques safe.

### When you get back

- Check your statements carefully for unfamiliar transactions.

## CHEQUE FRAUD

### Writing out cheques

- If you are making a cheque payable to a bank or a building society, do not make the cheque payable simply to that organisation. Add further details in the payee line, for example XYZ bank, re J Jones, account number XXX. If you try to deposit a cheque in a branch, or by post, made out simply to a bank or building society, it may be returned without processing.
- You should draw a line through unused spaces so unauthorised people cannot add extra numbers or names. It is also good practice to include the word 'only' after writing the amount in words.
- If it is necessary to make amendments, these should be made clear by crossing through the error and initialling or signing the correction.
- Never sign blank cheques.
- When writing cheques, be sure to complete all sections, including the payee name, and the amount in both words and figures.
- Always be sure to date cheques when you issue the cheque – undated cheques are likely to be returned with a request to include a date, as are post dated cheques. Alternatively they may get into the clearing cycle ahead of the specified date and money will be taken from your account before you intended it to be.
- Ensure you write your cheque using a ball point pen or indelible ink as this helps prevent cheques from being fraudulently altered.

### Receiving a cheque or banker's draft

- Never accept a cheque from someone unless you absolutely know and trust them. Be especially wary when accepting a high-value cheque or banker's draft.
- Be aware that a banker's draft or banker's cheque is not safe from fraud. If you receive a banker's draft or banker's cheque in payment for goods, you must allow time for it to clear before releasing the goods. A banker's draft or banker's cheque can be stolen or altered like any other cheque, and if it is altered, stolen or counterfeit it will not be honoured.
- Be aware that, even after the value of the cheque or banker's draft has been credited to your account, there is a risk that the money could be reclaimed if the cheque or banker's draft subsequently turns out to be stolen or counterfeit. At the end of six working days from paying in the cheque, you can be certain that the money is yours, and you are protected from any loss should the cheque turn out to be fraudulent (unless you are a knowing party of the fraud).
- Cheques should be paid into your account as soon as possible after receipt to reduce the risk of loss or theft, and should always be paid in within six months as older ones may be returned unpaid.

- The golden rule is that if it seems too good to be true, it probably is. Never accept a cheque from someone unless you absolutely know and trust them, particularly if you are selling high-value goods such as a car; ask for an alternative payment method such as automated phone payment, internet payment, Bacs payment (which takes three working days) or a CHAPS payment (a same-day service).



### Cheque Fraud

Losses from cheque fraud are decreasing, and the industry stops 90% of attempted fraud as the cheques pass through the clearing process, but if you use cheques regularly you should still take care.

There are three main kinds of cheque fraud in the UK: counterfeit, forged or fraudulently altered. For the most part, innocent victims who have had their cheque book stolen can expect to be refunded by their bank. However, you should be aware of scams that may leave you vulnerable.

- **Counterfeit cheque** – A cheque manufactured or printed on non-bank paper to look exactly like a genuine cheque and drawn by a fraudster on a genuine account.
- **Forged cheque** – A genuine cheque where part or all of it has been completed by a fraudster.
- **Fraudulently altered** – A genuine cheque where part or all of it has been altered by a fraudster.

Criminals are clever in using the clearing cycle to trick people into accepting forged, counterfeit or fraudulently altered cheques which then bounce.

## ONLINE

### How to protect you and your computer

- Install and maintain a firewall to protect your computer from unauthorised access by others. A suitable security software package will include this facility.
- Install and maintain anti-virus software, and set it to automatically scan your computer and all of its files on a regular basis. Also, make sure it is set to scan all files on your computer as they are opened, in particular those you receive as email attachments. A suitable security software package will include this facility.
- Install and maintain anti-spyware and anti-adware software, and set it to scan your computer automatically on a regular basis. A suitable security software package will include this facility.
- Set up your computer to receive all updates to your browser, operating system and software automatically, in particular your security software referred to above.
- Set your browser security settings to the highest possible level which will allow you to continue using the internet as normal without blocking access. For guidance on how to do this, refer to the Help section of your browser.
- If you use a home wireless network, you should make sure your hub is secure by installing a Wi-Fi Protected Access (WPA) system. Also, make sure you enable any integrated firewall capabilities which may exist on the hub. Consult your Internet Service Provider and/or hub manufacturer for further details.

By following the simple steps outlined here you will reduce your chances of becoming a victim of potentially dangerous viruses, programs and fraudulent scams.

## PHISHING EMAILS

Phishing is a process used by fraudsters to acquire sensitive information such as usernames, passwords and credit/debit card details by pretending to be a trustworthy company. Such communications claiming to be from banks or building societies are commonly used to trick people.

Phishing is usually carried out by email or instant messaging and often directs users to enter details at a fake website which looks almost identical to the real one.

Cumberland Building Society will never send you an email to your personal email address (e.g. yourname@yahoo.co.uk, yourname@hotmail.co.uk) unless in response to an email you have sent.

**If you believe you have disclosed personal security details on a phishing site, you should contact us immediately.**

## INTERNET BANKING

For advice on how to protect yourself from being a victim of fraud, when using Cumberland Internet Banking, please read the 'Safe and Secure use of Cumberland Internet Banking' leaflet a copy of which will be supplied to you when you register for Cumberland Internet Banking.

## ONLINE SHOPPING FRAUD

As internet shopping becomes more popular, the risk of being targeted by fraudsters also increases. Millions of people buy online every day without any problems. Being aware of potential scams, could help you avoid these problems.

### What are the risks?

- Buying goods that aren't delivered.
- Goods which don't match the original description.
- Delays and problems with online purchases.
- Poor after-sales service.
- Misuse of your card details.

### How can you protect yourself?

By following 3 simple rules, you can help to avoid being a victim of online shopping fraud:

#### 1. Deal with reputable sellers

- Look for evidence of a physical address and telephone contact details.
- Pick good sellers, especially when buying from private individuals.
- Check the sellers' privacy policy and returns policy.
- Be especially cautious when buying from overseas companies.

#### 2. Use a secure website

- Make sure you use a secure site to enter card details. Look for the padlock symbol in the browser window and for the website address to begin 'https://'.  
• Click on the padlock to check the seller is who they say they are.
- If you get a warning about a certificate be very cautious before continuing.

#### 3. Beware of scams

- Cross-check information on the internet and see if anyone else has experienced problems.
- Beware of 'work from home' scams which promise easy profits but never pay.
- Buy from reputable companies.
- Be extremely wary of anything that is offered in a spam email.

If you believe you have become victim to online shopping fraud, please contact us immediately.

**REMEMBER IF A DEAL LOOKS TOO GOOD TO BE TRUE, IT PROBABLY IS.**

## IDENTITY THEFT

Identity theft is one of the fastest-growing frauds in the UK. It happens when someone steals your name and personal details, then uses the information for their own benefit. The results can be devastating.

### How can a fraudster use your information?

Once a thief has your information they can:

- Open new credit card or bank or building society accounts, and run up debts in your name.
- Take out retail credit or loans in your name to purchase goods.
- Set up new telephone and internet services in your name.
- Change the billing address for your accounts, so you don't know there's a problem.
- File for bankruptcy in your name to avoid paying fraudulent debts.
- Apply for a new passport or identity document, then use your identity as a cover for criminal activity.
- Give your name to the police if arrested – if they are then released on bail, any further arrest warrants will appear in your name.

### How can you protect your identity?

- Ensure you shred any documents that include your name, address or any financial details.
- Be wary of any unprompted phone calls or emails, which appear to be from your bank or building society. You should never reveal your full passwords, login details or account numbers.
- If you are concerned about the source of a call, hang up and call them back using a legitimate number listed in the directory.
- If you move house, always get the Royal Mail to redirect your post.

You can check your ID has not been stolen by checking your credit reference with:

Experian [www.experian.co.uk](http://www.experian.co.uk) or

Equifax [www.equifax.co.uk](http://www.equifax.co.uk) or

Call Credit [www.callcredit.co.uk](http://www.callcredit.co.uk) (there is a charge for this service)

### What if you're a victim?

- If you are the victim of card fraud the most you will normally have to pay is £50. However, if you have acted fraudulently or without reasonable care, for example, by keeping your PIN written down with your card, you will be liable for all the losses.
- If your card is used fraudulently but you still have the card in your possession you will not be liable to pay for any part of the losses, unless you have acted without reasonable care or we can prove you have been party to the fraud. You would probably still have your card in your possession if you are a victim of 'card-not-present' fraud i.e. Internet or telephone transaction.

- Report lost and stolen cards or suspected fraudulent use of your card account, to your bank or building society immediately. (Keep a note of your card issuers' telephone numbers so that you can report lost or stolen cards).

### Reducing your liability

The most you will normally have to pay if your card(s), PIN, chequebook are stolen, lost or used by someone else is £50.

You may however be liable for the full amount of any losses if you have acted fraudulently or without reasonable care. Examples of what we will treat as not taking reasonable care includes –

- Keeping your chequebook and cards together.
- Allowing someone else to use your card.
- Telling someone else your PIN, VbV password or internet banking logon details.
- Keeping your card and PIN together.
- Giving your card / account details to someone you don't know.
- Not securely destroying card receipts or other account details (e.g. statements).
- Leaving bags, purses or wallets unattended.
- Not contacting your bank or building society to report a loss or theft.

### MORE ADVICE

You'll find more helpful information about tackling fraud on these web sites:

- Action Fraud [www.actionfraud.org.uk](http://www.actionfraud.org.uk)
- Bank Safe Online [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)
- Building Societies Association [www.bsa.org.uk](http://www.bsa.org.uk)
- Association for Payment Clearing Services [www.apacs.org.uk](http://www.apacs.org.uk)
- The Home Office [www.identitytheft.org.uk](http://www.identitytheft.org.uk)
- Get Safe Online [www.getsafeonline.org.uk](http://www.getsafeonline.org.uk)
- Be Card Smart [www.becardsmart.org.uk](http://www.becardsmart.org.uk)

The Cumberland Building Society has no connection to the above sites and is not responsible for the contents of these sites.

By taking these simple precautions we trust you will have many trouble free years as a Cumberland customer.

## CONTACT US

Call our Customer Service helpline on 0845 601 8396 from 8am to 8pm Monday to Friday, 8.30am to 4.00pm Saturday, or 01228 547090 at all other times to:

- Report suspected fraudulent use of your card account
- Report lost or stolen cards

It is important that you inform the Society immediately.

If you think someone has discovered your PIN, or if you forget it, tell us immediately and we'll send you a new one. Just speak to your branch or call our Customer Contact Team on **0845 601 8396 or 01228 403141**.

This leaflet is intended to highlight what you can do to help us to protect you from being a victim of fraud.

Further information regarding your responsibilities and liability for any fraudulent withdrawals are provided in our Savings & Current Account Terms & Conditions and VbV Terms of Service, Cumberland Internet Banking Terms & Conditions and Card Conditions leaflet, copies of which are available from any branch of the Society.

INV407 08/11 V5

Cumberland Building Society, Cumberland House, Castle Street,  
Carlisle, CA3 8RX · Phone: 0845 601 8396 · 01228 403141  
[customerservice@cumberland.co.uk](mailto:customerservice@cumberland.co.uk)

To help us monitor and improve customer service telephone calls may be recorded.

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