HOW TO PROTECT YOURSELF FROM FRAUD

Essential information for your own protection

The Cumberland

CURRENT ACCOUNT SWITCH GUARANTEE

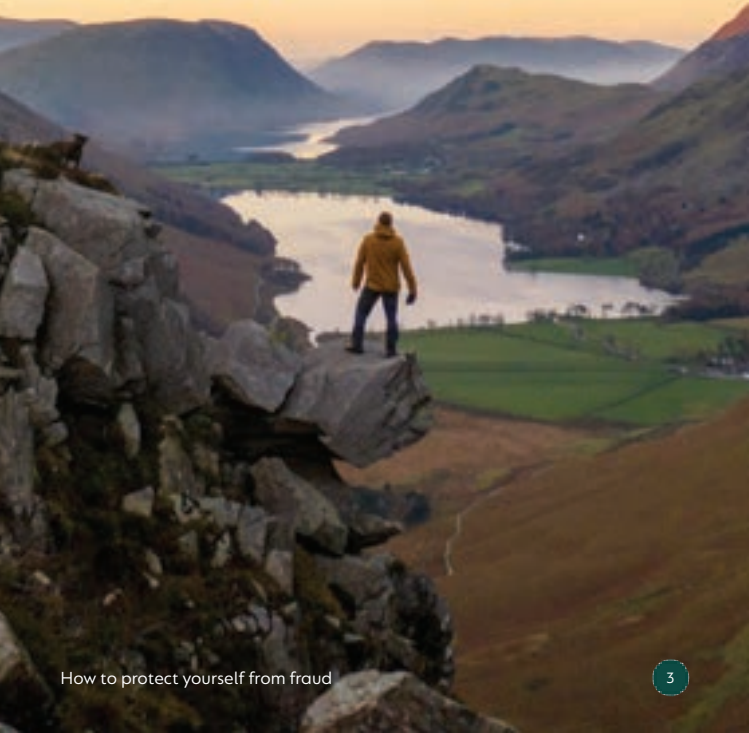
Pay

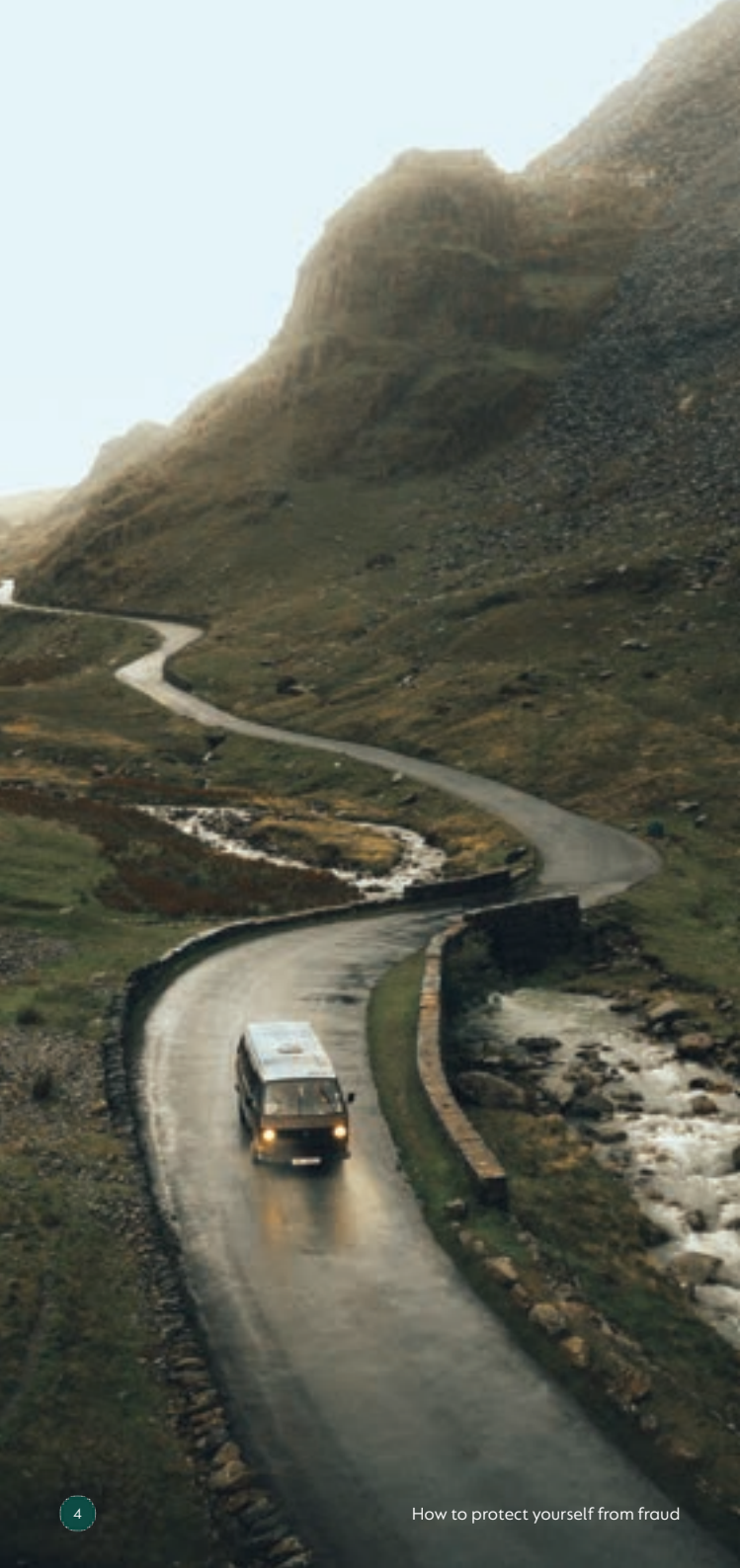
G Pay

WE TAKE FRAUD VERY SERIOUSLY AND DO A LOT TO HELP PROTECT YOU FROM FRAUD

This leaflet explains how you can help protect yourself from being a victim of fraud

CONTENTS





TOP TIPS

- **Cards:** Keep your cards safe and never leave them unattended.
- **ATMs:** Look out for anyone behaving suspiciously and for signs of tampering on the cash machine.
- **Passwords & Codes:** Never tell anyone else your PIN, password, access code or passcode, and never write any of them down in a way which could easily be understood by someone else.
- **Scams:** Be wary of unprompted phone calls, emails or text messages asking you for personal information such as your PIN, password, access code or passcode. We'll never call, text or email you asking for account information.
- **Watch Your Account:** Regularly check your account for unfamiliar transactions. Let us know immediately if you notice anything unusual, **call 01228 403141**.

THINGS WE'LL NEVER DO...

- Ask for your PIN, Internet Banking login details or One Time Passcodes
- Send someone to your home to collect cash, bank cards or anything else
- Ask you to authorise the transfer of funds away from your Cumberland accounts
- Ask for a One Time Passcode to cancel a transaction or authorise a refund

DEBIT CARD SECURITY

TAKE CARE OF YOUR CARDS

Keep Them Close: Don't let your card out of your sight when making a transaction.

Only You: Never allow someone else to use your card, not even your partner, family or friends.

Don't Be Distracted: Don't let anyone distract you when using your card and always put it away quickly afterwards.

At Home: If you live in a property where other people have access to your mail, you can ask us to make your card unusable until you call us to say you have received it.

Lost or Stolen: If your card is lost or stolen, report this to us immediately by calling us on **01228 403141**. If you call out of hours it is important that you leave a message on the answer machine. By doing so your liability for any fraudulent transactions ends at that point.

DEBIT CARD SECURITY

AT THE CASH MACHINE

Behind You: Be aware of others around you. If someone is close to the machine and behaving suspiciously or makes you feel uncomfortable, use another one.

Keep Your Eyes Peeled: If there's anything unusual about the cash machine or there are signs of tampering, don't use it and tell the building society, bank, police or building owner immediately.

Avoid Darkness: Avoid using cash machines in poorly lit or isolated areas.

Cover Up: Cover the keypad to avoid anyone seeing you enter your PIN.

Swallowed Card: If the cash machine doesn't return your card, tell us immediately.

DEBIT CARD SECURITY

PERSONAL CODES & NUMBERS

Don't write them down: Never write down or record your personal codes and numbers in a way that could easily be understood by someone else.

Tough To Guess: Never choose personal codes and numbers that could be easy for others to guess (such as your date of birth).

Keep Secret: Never tell anyone your personal codes and numbers. This includes family, friends, Cumberland staff and the police. You are the only one that should ever know them.

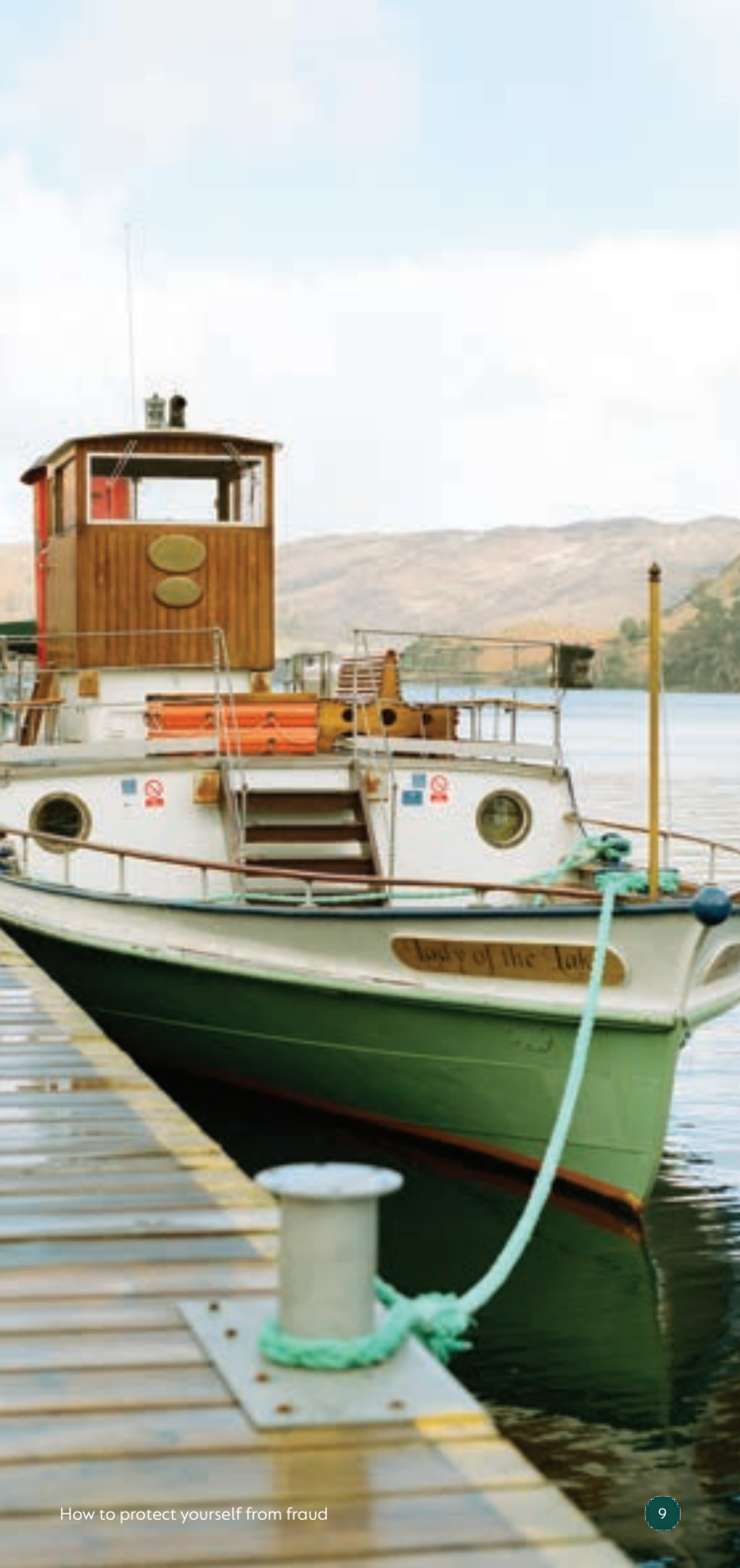
Keep Them Covered: To prevent anyone else seeing them, always cover your personal codes and numbers when entering them.

Card PIN and Phone: Never enter your PIN into a telephone keypad.

SHOPPING ONLINE

When you use your Visa debit card to purchase goods or services online, you may be asked to authorise the transaction using a One Time Passcode (OTP) which will be sent to your mobile. If you don't have your mobile number registered with us, you may not be able to shop online, so we recommend that you register a mobile number as soon as possible.

We will never ask you to share your OTP to anyone to verify your identity, stop a transaction or authorise a refund. An OTP will only ever be used to authorise an online purchase.



INTERNET BANKING AND MOBILE APP

USING INTERNET BANKING SAFELY

Use only Official Links:
Only log on from our website cumberland.co.uk (or cumberland.co.uk/business for businesses).

Enable Software Protection: Install firewall, anti-virus and anti-spyware software on your computer. Keep them, your operating system and browser up to date and carry out regular scans.

Use only Secure Wi-Fi: If you have your own wifi hub, make sure it's set up to be secure and password protected.

Avoid Public Internet: Don't use public computers to access Cumberland Internet Banking unless absolutely necessary. Always ensure your access details cannot be viewed by anybody else and you log out when finished.

Always Be Aware: Never log on to your Internet Banking if asked by a cold caller (for example, someone offering to fix, upgrade or protect your computer). Do not disclose any of your personal access information.

INTERNET BANKING AND MOBILE APP

USING OUR BANKING APP SAFELY

Enable Virus Protection: Check your mobile devices are protected against malware (malicious software) or viruses.

Add a Phone PIN: Set up a PIN, fingerprint or face ID on your mobile device. Don't store your passcode, password or access code on it. Don't share it with others.

Avoid Public Wifi: Avoid using public wifi. Disable Bluetooth when using our app.

Use only Official App Stores: Only ever download our app from the official app stores: iTunes or Google Play.

Don't Tamper with Your Device: Don't install the app on a rooted or jailbroken devices, in other words a phone that has had its default operating system restrictions removed.

SCAMS TO BE AWARE OF

CRIMINALS ARE USING A VARIETY OF TACTICS INCLUDING FAKE EMAILS, PHONE CALLS, TEXTS AND SOCIAL POSTS TO OBTAIN YOUR BANKING DETAILS.

NUMBER SPOOFING

Fraudsters will make it appear that they are phoning from a number of a genuine bank or building society.

A common scam involves someone claiming to be calling from the fraud team to advise there is fraudulent activity on your account. The call is likely to follow this pattern:

They sound genuine and often advise you to check the number they are calling from to create a false sense of security.

The fraudster will then ask you to confirm your banking details. They may already be aware of some of your details or ask you to confirm the last digits of your card.

They also ask for One Time Passcodes, saying this is to either verify your identity or cancel a fraudulent transaction.

We would never ask you to disclose any card details or Internet Banking details to cancel a transaction.

SCAMS TO BE AWARE OF

DELIVERY COMPANY AND PHONE PROVIDER TEXTS

Fraudsters often send texts, which appear to have been sent by genuine organisations such as delivery companies or phone providers requesting you to update payment details.

A delivery scam works like this:

- The scammer will pressure you to click a link, included in the text, to provide banking details.

If this information is given, it can be used either to take fraudulent card transactions or to identify who you bank with and then target you with number spoofing.

A genuine company would never send a link via text and ask you to update payment details.

FAKE WEBSITES

Fraudsters will often use fake websites which appear to be genuine organisations to get customers to contact them. For example, fake Paypal and Amazon websites appear high on the search list on Google.

Always check the web link you are clicking on.

Log in to the company's website and contact them through your own account rather than through a number found online.

SCAMS TO BE AWARE OF

WHATSAPP AND SOCIAL MEDIA

Fraudsters will often hack social media accounts and send messages to friends or family asking for emergency money. The messages appear to be genuine as they come from a known person's account.

Always phone the person first to make sure the message is genuine.

Fraudsters will also contact you via Whatsapp or text message claiming to be your son/daughter saying they have a new new phone and have an urgent payment to make however, because they are on a new phone they are unable to access their own Internet Banking.

The messages never address you by name and will usually address you as "mum" or "dad".

These messages will be sent to hundreds of people. Eventually, someone will respond.

Again we recommend contacting the person they are claiming to be on a number you already have for them and not the new number.

SCAMS TO BE AWARE OF

INVESTMENT SCAMS

There is a huge increase in investment scams relating to Bitcoin or other digital currencies and will often claim to be endorsed by celebrities. If you are looking to invest, we urge you to research any firm and any financial advisors.

Search the company on the registers of the official regulator, the Financial Conduct Authority (FCA). You can check they are a regulated firm here.

Search the company on Companies House.

There may be restrictions on withdrawals. Make sure your expected returns are realistic: past performance is no predictor of future performance. Your capital is always at risk.

ROMANCE FRAUD

Fraudsters will use social media platforms, dating sites and online gaming to speak to people over long periods of time to gain their trust. Eventually, they will either directly ask for money or put you in a position where you want to help and offer to send them money.

Never send money to someone you have only spoken to online and never met in person.

IF A FRAUDSTER TAKES MONEY FROM YOUR ACCOUNT, WE'LL REFUND THE TRANSACTIONS TO YOUR ACCOUNT SO IT'S LIKE IT NEVER HAPPENED.

This includes refunding any charges and interest you've incurred, and paying any interest you've missed out on.

You may however be liable for the full amount of any losses if you've acted fraudulently or with gross negligence (for example, allowing someone else to use your card, telling someone else your personal information, keeping your card and PIN together, not contacting us immediately to report a loss or theft, or leaving bags, wallets or purses unattended).

You must tell us immediately if you notice any unauthorised transactions on your account, or if your debit card is lost or stolen.

OUR PROMISE TO YOU

KEEP YOUR CONTACT DETAILS UP TO DATE

If we spot unusual transactions on your account, we'll contact you by phone or text to check these with you. We may need to send a One Time Passcode (OTP) to your mobile number when you're shopping online. It's therefore very important that we have your up to date telephone numbers on our records. You can update your contact details by:

- visiting your local branch
- writing to us at the address on the back of this leaflet
- going to the "Change My Contact Details" page on Internet Banking
- calling us on 01228 403141
- completing the "Change My Details" form available on our website and sending it to us by post or as a scanned email attachment to **changemydetails@cumberland.co.uk**

Note that we need your signature in order to update your mobile phone number.

THE FOLLOWING WEBSITES CONTAIN IMPORTANT INFORMATION ON PROTECTING YOURSELF AGAINST FRAUD AND IDENTITY THEFT.

getsafeonline.org
- a site which gives valuable advice and information about internet safety.

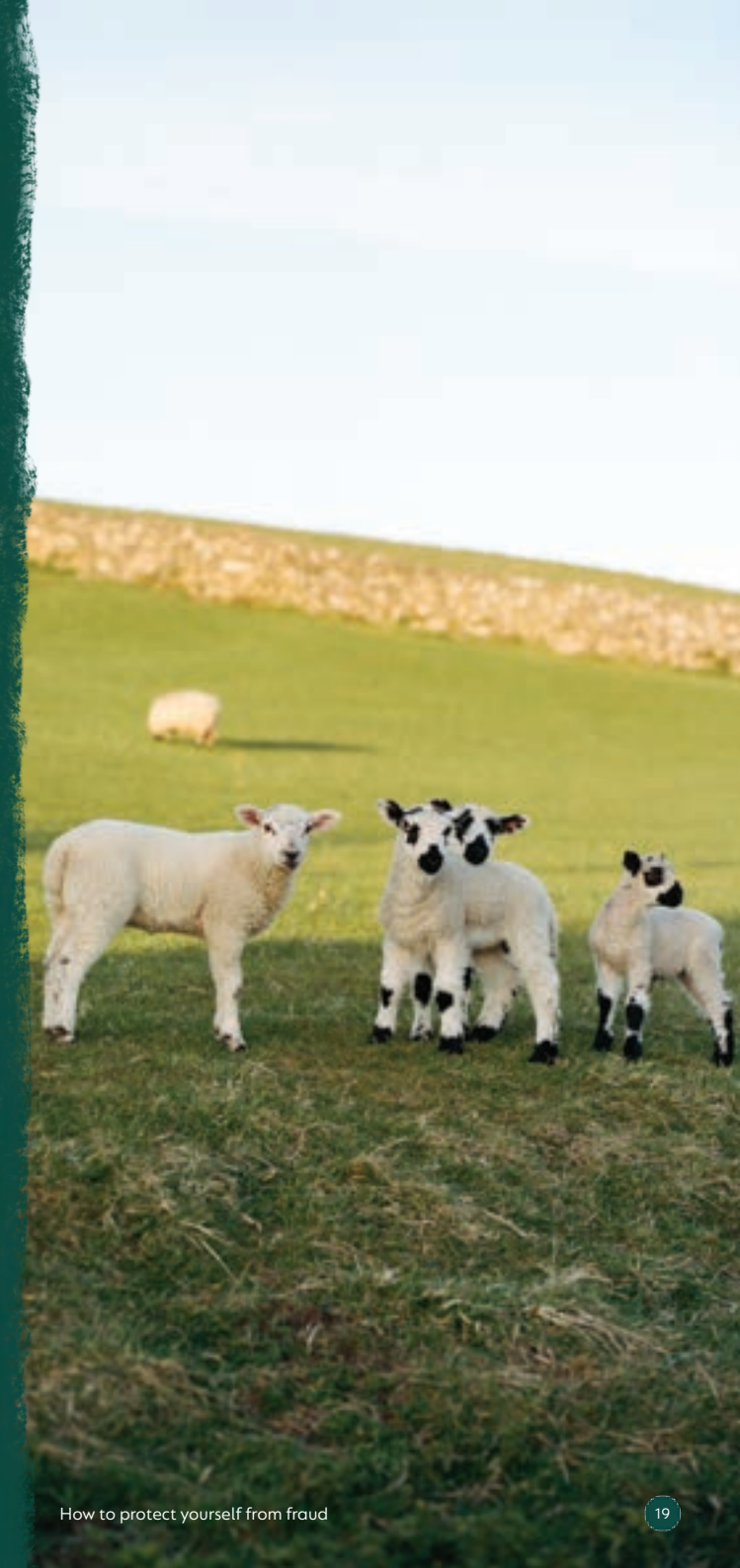
actionfraud.police.uk
- a site provided by the National Fraud Authority, the government agency that helps to co-ordinate the fight against fraud in the UK.

financialfraudaction.org.uk
- simple advice from Financial Fraud Action UK on how to stay safe when shopping online.

fca.org.uk/consumers/scams
- The Financial Conduct Authority (FCA) site that provides guidance on how to avoid scams.

takefive-stopfraud.org.uk
- straight forward advice to help you protect yourself from preventable financial fraud and scams.

The Cumberland is not responsible for the content of these external internet sites.



CURRENT ACCOUNT SWITCH GUARANTEE

Cumberland Building Society
Cumberland House, Cooper Way,
Parkhouse, Carlisle, CA3 0JF

Phone: **01228 403141**
help@cumberland.co.uk
cumberland.co.uk

The Cumberland

recycle
INV407 v11 01/23