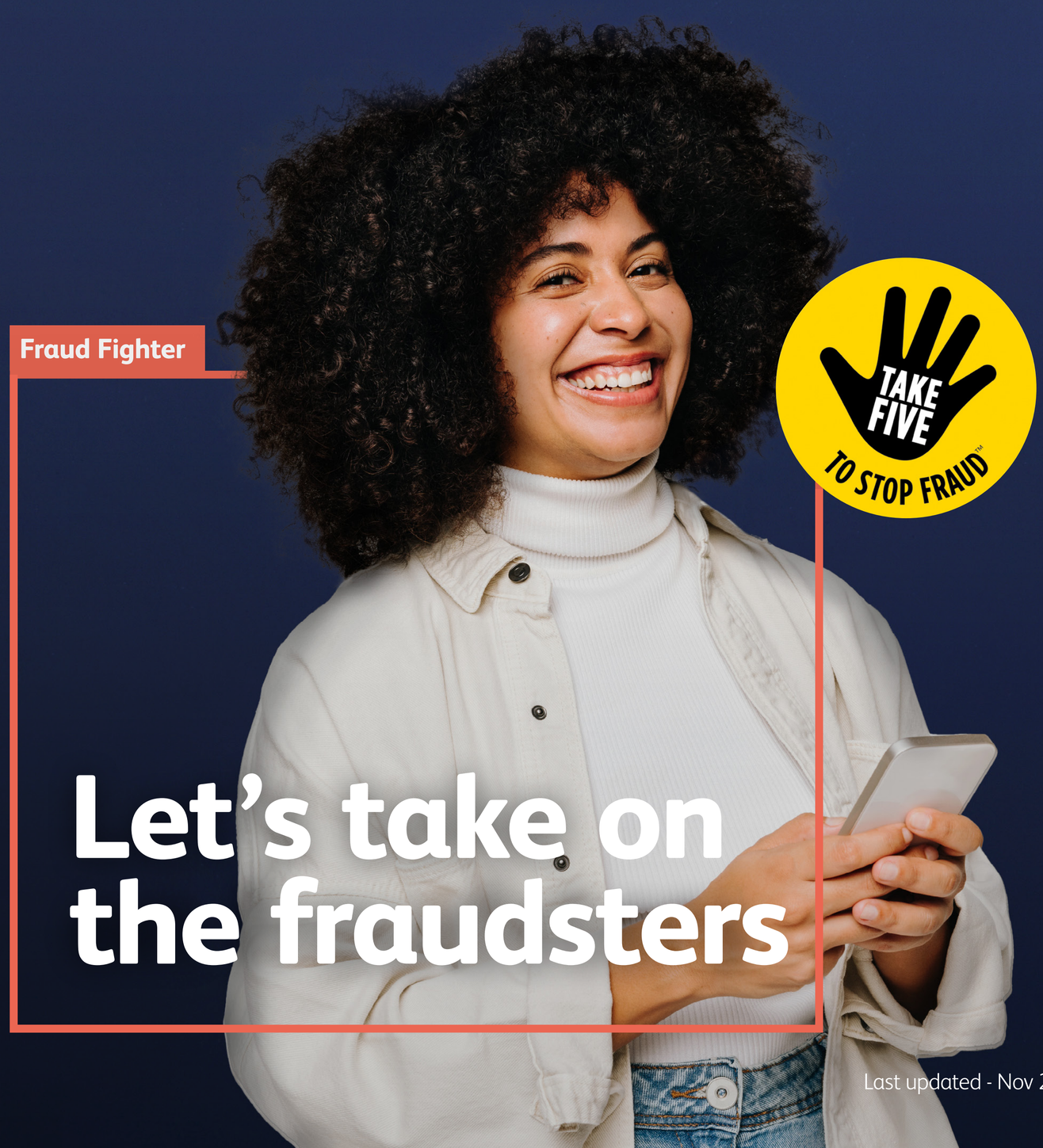
The co-operative bank

Ethical then, now and always

Protect yourself from fraud

Fraud advice booklet



Last updated - Nov 2023

Contents

This document is interactive.
Use the top navigation to jump to any section.

Helping you spot the warning signs of fraud *3*

Impersonation Scams – the police or your bank *4*

Impersonation Scams – Utilities or Broadband Scams *5*

Investment Scams *6*

Purchase Scams *7*

Courier Fraud *8*

Fake Emails and Texts *9*

Money Mules *11*

Doorstep Scams *12*

Online Dating and Romance Scams *13*

Invoice Scams *14*

Lottery and Prize Draw Scams *15*

Take Five *16*

Useful Links *17*

Helping you spot the warning signs of fraud

Fraud crime is growing, and becoming more sophisticated. So it's very important that you know about it. No matter your age, wealth, or wellbeing, fraudsters will target you.

They use all kinds of methods to get hold of people's money. They might pretend to be the police, or even say they're calling from your bank. But there are ways to spot them, and stop them in their tracks.

This guide highlights some of the most common scams and warning signs you need to look out for.

This type of crime can cause devastating effects to people and their families.

Don't let it happen to you.

Fraud Guarantee

Our Fraud Guarantee means that if you fall victim to fraud, we guarantee to refund your loss as long as you've not acted fraudulently and have taken reasonable steps to keep your details safe.

Pretending to be the police or your bank

Trusting people is something we all do instinctively, and when someone calls you out of the blue, saying that they are from the Fraud Department of your bank, or even the police, you should trust them right? Wrong!

Criminals will call you pretending to be from your bank or the police. They catch you off guard, claiming that fraudulent activity has been spotted on your account or that they are concerned about the safety of your money. They use a number of techniques, pressuring you into doing what they ask and before you know it, they've stolen your money.

How does it happen?

- You receive a call out of the blue from your local 'police' and they'll tell you that they suspect fraud has occurred on your bank account. They will ask you to help with their investigation and to move your money to another account to 'keep it safe'. They'll ask you to withhold from telling your bank the real reason you are moving your money as the bank could be involved. Moving this money is a trap and would result in your money being stolen by a fraudster.
- Another twist on this type of scam is when they call pretending to be from the Fraud Department of your bank, asking you again to move your money to keep it safe.

Protect yourself - Think scam!

- Be vigilant, the police or the bank will never ask you to move your money out of your account to keep it safe or ask you to visit a branch and take out cash to hand over to them.
- The police or bank will never ask you to assist with an investigation.
- If you have been instructed to tell the Bank, when questioned, that you are moving your money for a different reason or you have been told not to trust us, then stop! It's a scam!
- Contact your telephone service provider to discuss call-blocking solutions.
- Remember, criminals can easily manipulate the number that is shown on a telephone caller display in order to look genuine.

Remember:

If you receive a call:

- ✕ **Never share your bank account or security information in full**
- ✕ **Never share the PIN for your card with anyone**
- ✕ **Never tell anyone your Online Banking One Time Passcodes that we send to you in a text or an email. Not even us!**
- ✕ **If we suspect fraud on your account we may send you a message to check it was really you making the payment.We will never call you and ask you for any details from this message or tell you how to reply to it.**

Impersonation Scams – Utilities or Broadband Scams

Criminals will call you out of the blue, pretending to be from trusted broadband providers like BT, TalkTalk, Sky, or even Microsoft. They'll claim that they are calling in relation to issues with your broadband, but the steps they take you through to 'fix' the problem, lead to you losing your money.

How does it happen?

- One example of this scam is that you receive a call telling you that there is an issue with your broadband. They tell you they can fix it either by clicking on a link in an email, or by downloading an app to your device that allows them access to your device remotely. The link or app gives criminals complete control of your computer.
- They'll spend hours on the phone with your pretending to resolve the issues, asking you to log in to your emails and online banking to check everything is working ok. They may even offer you 'compensation'. They'll then say that they've accidentally credited you with too much money and ask you to send it back urgently. You log on to your online account, but as the criminals have access to your device, they trick you with fake screens to make you think there is a problem or making you think they've compensated you with too much money. In reality, they have moved your savings to your account and without realising you send it all to the criminal.
- Another twist on this scam is that the caller pretends to be from a trusted retailer, like **Amazon**, telling you that you're due a refund and you need to check that you've received it, or they may pose as someone from **HMRC** threatening prosecution for unpaid taxes.

Protect yourself - Think scam!

- **Never** agree to download an app or software on your mobile or computer following unexpected contact. The bank, the police or any other trusted organisation would never ask you to do this!
- Be very wary of out-of-the-blue phone calls. If you're unsure if you are speaking to the genuine company, put the phone down immediately and don't answer any further calls from them. Contact the company directly using a number from a trusted source, such as their website and call them back, ideally from another phone to check if the caller was genuine.
- It may be a coincidence that you are having problems with your broadband. If you are, call them directly yourself for advice or support. That way, you know that you have started the conversations.
- Contact your telephone service provider to discuss call-blocking solutions.

Remember:

If you receive a call:

- ✕ **Never share your bank account or security information in full**
- ✕ **Never share the PIN for your card with anyone**
- ✕ **Never tell anyone your online banking verification or token codes. Not even us!**

Investment Scams

Investing in stocks, bonds and shares or any other commodity can be a successful way of making money, but it can also lead you into losing your entire life savings, especially if it's a scam.

Criminals will try to trick you into investing in a 'risk-free, once-in-a-lifetime opportunity, guaranteed to soar in value'. They'll use professional-looking websites and legitimate-looking social media pages to entice you.

How does it happen?

- You're searching for an investment online or see an advert offering an opportunity to make a lot of money – fast!
- The website that you visit looks very professional and you ask for more information. You'll receive glossy marketing material but will soon be bombarded with phone calls and emails warning and pressuring you not to miss out on the deal.
- Enticed by the offer, you invest your savings and wait to see the return on your investment. At first, some criminals will offer you a small return to trick you into investing more, but then all contact stops and your money has gone.

Protect yourself - Think scam!

- Remember, there are no get-rich-quick schemes. **If it sounds too good to be true, it probably is.**
- Do some research! Many of these fake investment companies will be overseas and won't be authorised by the Financial Conduct Authority. Criminals can even clone a legitimate firm. Check the FCA's warning list on their website fca.org.uk/scamsmart/warning-list
- Legitimate companies won't pressure you. Don't be afraid to say 'no'. Be firm, hang up and don't respond to any more emails. Never sign up to anything immediately. **Always seek independent financial advice.**
- Search for reviews about the company to see if there is any reference to it being a scam.
- Call the company directly using the telephone details that are held on the FCA website to check that the person you are dealing with actually works for them and that they are genuine.
- Stay in control of your trading accounts and wallets and avoid letting a 'trader' set up or control your account. Don't share your card details or download software on your device that allows someone to access remotely and control your trading account.
- Crypto investments are considered high risk. You can check the FCA website for unregistered cryptoasset businesses that are operating in the UK. Visit fca.org. uk/consumers/cryptoassets

Purchase Scams

Online shopping can save you time, effort and money. Those great deals can tempt anyone to take a greater risk if they think they're getting a bargain, and criminals know it!

Fraudsters will try and trick you through fake adverts, websites, social media accounts and emails, advertising goods or services that don't exist or aren't even theirs to sell.

How does it happen?

- You receive an email, or see an advert when searching online or through social media, advertising a special offer or a deal you like the look of and you click on the link.
- The webpage that you visit looks authentic, it can appear to belong to a well-known brand or high-street chain, or seems to be a genuine company you'd like to try for the first time.
- Enticed by the offer, you purchase the goods, but they never arrive. You call and email the seller/company, but nobody replies. You've lost your money!

Protect yourself - Think scam!

- Be cautious. Never click on a link in an unexpected email and be cautious when clicking on adverts online or via social media.
- Avoid paying by transferring money straight from your bank account. Using your debit or credit card offers more protection when purchasing goods.
- Do some research - check out the seller to be confident they're genuine and try a number of review sites for other shoppers' opinions on their quality of service.
- If you're buying high-value items, it's better to view them in person before parting with any money.

Courier Fraud

While many criminals rely on the anonymity of the telephone and internet to scam their victims, with a courier scam, they'll come to your home.

How does it happen?

- They will initially contact you by telephone, pretending to be from your bank or the police. They'll tell you that they are carrying out an internal fraud investigation at the bank and need you to assist them.
- They'll ask you to go to your local branch and withdraw a large amount of cash to hand over to them when they come to your home. They will tell you that it is an undercover investigation to convince you not to tell the bank why you're withdrawing the money.
- They'll tell you it's to allow them to check if the money issued by the bank is counterfeit, or that they're going to keep it safe while the investigation is underway.
- They may even ask you to buy high-end jewellery or goods to see if the notes are accepted and then they'll come to collect it from you.
- In some cases they may also come to your home to collect your card and PIN.

Protect yourself - Think scam!

- Be extremely wary of calls out of the blue. The bank or police will **never** ask you to assist them with an investigation. We will **never** arrange to come to your home to collect your cash, card or PIN.
- If you are called out of the blue, end the call immediately. Ignore any further calls and try to contact the bank on the telephone number from the back of your bank card. Ideally, use a different phone to call us in case the criminals are waiting on the line.
- Speak to your family, friends or neighbours before doing anything.
- If you think you are being scammed and have already given the criminals your home address, call the police immediately. Then contact us so that we can protect your account.

Reporting fraud to Action Fraud

Reporting online: actionfraud.police.uk

Telephone reporting: 0300 123 2040*

Fake emails and texts

Many victims of fraud and scams wonder how the criminals managed to get hold of their personal or financial information.

They do this through sending out mass volumes of fake emails and text messages in the hope that someone will respond and give them the information they need. The messages will be riddled with links or telephone numbers all designed to gather your information.

How does it happen?

You receive a fake email or text message from a well-known parcel delivery company claiming that they have been unable to deliver your parcel. You're asked to click on a link to arrange for the parcel to be delivered and will be asked to confirm your personal or financial information. Once the criminal has this, they typically use this information to scam you days, or weeks, further down the line. They may call you impersonating trusted organisations, or they may use the information to gain access to your bank account or to even use your card details fraudulently.

There are wide variety of fake emails and text messages distributed by criminals with common asks of you, such as:

- Friend/family in need texts and WhatsApp messages claiming their mobile number has changed and going on to ask for financial help
- Pay immediately!
- Complete this form
- Sign up here
- Verify your security or log in here
- Contact us on...

Protect yourself - Think scam!

- Be very wary of unexpected emails and text messages and avoid sharing your personal or financial information via email.
- Never click on a link in an unexpected email that asks you to 'log in' or 'pay now'.
- Stop and think, don't respond immediately. To check if it is genuine, we advise you to contact the company directly using a telephone number from their genuine website.
- Look out for some simple signs of a fake message:
  - They don't use your first name, instead they'll address you as 'Dear Customer' or use your full email address as your name.
  - The message is threatening or has a strong sense of urgency.
  - It may look like a genuine email address that has been changed very slightly to look similar e.g. Co-operativebank.co.uk
  - The email contains spelling errors or uses poor grammar.

If you have received an email that you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk.** Or, if you have received a suspicious email that is posing at The Co-operative Bank, you can forward it to **ihaveseenascam@co-operativebank.co.uk**

Money Mules

Criminals don't want to get caught. So they use or recruit other people to launder the profits of their crimes. These people are known as Money Mules.

Criminals will ask the Money Mule to receive the criminal funds into their bank account and to move it on. This is a criminal offence and has real consequences. While some Money Mules knowingly become involved in this type of criminal activity, many are completely innocent and totally unaware of where the money comes from or where it's going. But it could be used to fund drugs, child trafficking or terrorism.

How does it happen?

- You see a job advert in a newspaper, website or through social media offering work from home with the promise of fast cash for minimal effort.
- The job involves buying and selling products online, with money coming into your personal account, then being asked to send it on to another account by your employer, leaving you with a cut of the money.
- Criminals may just contact you directly and ask you outright to accept money into your account and to move it on, for a cut of the money.

Protect yourself - Think scam!

- Stop and think – don't give your bank account details to someone unless you know and trust them.
- Don't accept money into your account and agree to move it on for somebody if you don't know the person and don't know where the money is coming from.
- Be wary of job offers where all interactions and actions are completed online.
- If the job seems too easy and the money you earn seems too good to be true – it probably is.
- If you become a Money Mule, your bank account will be closed, you will have problems applying for bank accounts, loans and credit cards in the future and will even find it difficult to get a phone contract. Worse still, you could go to prison for up to 14 years.

Doorstep Scams

This type of scam involves criminals knocking on your door unexpectedly, offering to sell you goods or services. The goods may be overpriced, poor quality or even stolen. More commonly, they may pretend to be workmen telling you that they've noticed urgent work needs to be carried out on your home.

How does it happen?

- They'll knock on your door, posing as a builder. They'll tell you that they're working in the area and they've noticed you need urgent repair work to your home. It's typically your roof in the hope that you can't get up there to see the damage.
- They may carry out further inspections in the loft and on the roof, using pictures of any damaged roof to convince you it's yours.
- They'll tell you they're only in the area for the next few days and that if you can get them the cash, they'll get the work done immediately. They may even offer to take you to your local branch.
- If you give them the cash in full, they probably won't return. In some cases, they'll pretend to carry out the work, taking small payments from you for materials and then find more and more problems, to steal more of your money.
- To avoid suspicion, they may tell you to tell staff in the branch that the money is for another reason.

Protect yourself - Think scam!

- Be very wary if somebody knocks on your door unexpectedly.
- Some callers may be legitimate, such as from gas, electricity or water companies. Always ask for identification before letting them into your home. Call the company to check their ID using a trusted number from their website or a recent bill. Don't call the telephone number on the ID card.
- If you need work carrying out on your home, get a number of quotes from other reputable tradesmen before agreeing to the work. Don't pay in full and avoid paying in cash. It's safer to transfer the money from your bank account and this also provides a trace of the payment.
- Do some research on the builder or company that you're speaking to. A simple search of their name on the internet may provide reviews from other customers or highlight if they are rogue traders.

Online romance Scams

Online dating and the use of social media sites such as Facebook is a popular way to meet new people, with millions of people finding new friendships and romantic relationships in this way.

Among the genuine profiles on these websites are fake ones set up by criminals, and unfortunately they want your money. They are master manipulators, they'll spend months playing on your good nature, your emotions and even your vulnerabilities so they can steal your money.

How does it happen?

- You meet someone online and you seem to have a lot in common. You quickly build up a relationship before they ask you to move the communication away from the dating website or social media page, allowing them to email you directly or even text or call you.
- They'll flatter you, make you feel like they're really interested in you and before you know it, you're in love.
- They won't ask for money immediately, initially they may start to talk about financial issues in the hope that you will feel obliged to help. They may say they need money for a travel ticket to come and meet you, but suspiciously the arrangements fall through. They may mention a family emergency or a problem with their business. Before you know it you've sent them money many times, before eventually they cease all contact with you.

Protect yourself - Think scam!

- Don't be convinced by the profile picture – it's probably fake! Criminals talk to you online because it's anonymous, so you won't be able to identify them. You can check photos using a reverse image search on the internet through websites such as **tineye.com.**
- If they avoid meeting you in person or letting you see them face to face in a video call, it's the sign of a scam.
- Avoid sending money to someone you haven't met in person and be wary of giving money to someone you don't really know.
- Never agree to receive money on behalf of them and agree to transfer it on. They may be using you to launder money, which is a criminal offence.
- Talk to your family and friends for advice. If the person you're talking to online asks you to keep the relationship and requests for money a secret, then it's more than likely a scam.

Invoice Scams

Invoice scams happen when criminals trick you in to sending money to them by posing as solicitors, tradesmen or someone from a trusted company who you may have genuinely received goods or services from.

How does it happen?

- You receive an email from a solicitor instructing you to make a payment to secure the purchase of your new home. The email provides you with the sort code and account number for you to make the urgent payment to.
- You make the payment that day and respond to the solicitors email confirming that you've made the necessary payment. Having heard nothing back, you call them to find out what's happening.
- They advise that they never sent the original email and upon further investigation it is confirmed that their email account has been hacked by a criminal and the account details provided belong to an account controlled by them.

Protect yourself - Think scam!

- If you receive an email requesting for payment for goods or services you've received, providing you with new or amended bank details, it's important that you call the person or company first to check that the request is genuine and that the account details are correct.
- Call them using trusted contact details, such as from their website, and avoid using the telephone numbers within the email. This could lead you to call the criminal.
- Always question changes to bank details. Genuine companies rarely change their bank account details.

Lottery and Prize Draw Scams

You may receive a letter, telephone call or email announcing that you've won a foreign lottery that you've never heard of, let alone entered. You may also be told that you've won a promotional prize. While the offers sound convincing, most of them come from criminals who are trying to trick you into paying them money and revealing your personal information.

How does it happen?

- Congratulations! You receive an email or letter telling you that you've won a huge amount of money in a lottery or a prize is waiting for you!
- You're told that to claim your winnings, you need to send money to cover 'processing' or 'administration' fees or taxes.
- Enticed by the offer, you send them the money, including your personal information and bank account details.
- You never receive your winnings, they steal your money and your information, which is then used to target you with further scams.

Protect yourself - Think scam!

- Stop and think – ask yourself, how could you win a lottery if you've never entered it or bought a ticket?
- If you've won a prize, you shouldn't have to pay to receive it!
- **Never** share your personal or bank information with anyone unless you're sure you know who you're dealing with.
- If you are receiving spam mail through the door visit **friendsagainstscams.org.uk** – a National Trading Standards campaign for more advice.

Take Five to Stop Fraud

Take Five to Stop Fraud is a national campaign led by UK Finance and backed by the Government. The campaign offers straightforward and impartial advice to **help everyone protect themselves from preventable financial fraud.**

Many people may already know the dos and don'ts of financial fraud and scams. The trouble is, in the heat of the moment, it's easy to forget this.

After all, trusting people on their word is something everyone tends to do instinctively. If someone says they're from your Bank or a trusted organisation, why wouldn't you believe them? Take Five urges you to stop and consider whether the situation is genuine – to stop and think if what you're being told really makes sense.

To learn more about this national campaign visit:
takefive-stopfraud.org.uk

STOP

Taking a moment to stop and think, before parting with your money or information, could keep you safe.

CHALLENGE

Could it be fake? It's OK to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT

Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud:
actionfraud.org.uk

Useful Links

As your bank, it's our job to arm you with the information you need to protect yourself from fraud. By keeping your guard up, and following some simple rules, you can spot the warning signs and keep your money safe.

For more information about fraud, please visit the links below.

If you're ever in doubt, or feel under pressure, then it's probably a scam.

The Co-operative Bank Fraud Guarantee

Our Fraud Guarantee means that if you fall victim to fraud, we guarantee to refund your loss as long as you've not acted fraudulently and have taken reasonable steps to keep your details safe.

Visit our website:
co-operativebank.co.uk/global/security

Financial Conduct Authority:
fca.org.uk/scamsmart/warning-list

or call the FCA consumer helpline on: 0800 111 6768*

Take Five to Stop Fraud awareness campaign:
takefive-stopfraud.org.uk

Don't Be Fooled:
moneymules.co.uk/

Scams are fraud and fraud is a crime – report it!

It's understandable to feel embarrassed if you've been the victim of a scam.

Many victims say that they can't believe they fell for it, or that they feel foolish. The truth is, these criminals are master manipulators; they use complex techniques to trick people and steal their money and they're good at it! Billions of people fall victim to scams and fraud every year and it's important that these scams are reported as soon as possible.

The sooner it's reported, the quicker we can start the investigation and try to get your money back. **If you think you've been a victim of a scam or are currently being scammed, report it to us immediately.**

We've partnered with Stop Scams UK to provide the 159 service to our customers. This provides a vital route back to safety for people who are at risk of being manipulated and scammed by fraudsters.

If you believe you are being targeted or have been a victim of a scam call 159 where you'll be safely routed through to us.

Please call +44 (0) 3457 212 212* (Lines open 8am to 6pm Monday to Friday, 9am to 5pm Saturday and Sunday) if you would like to receive this information in an alternative format such as large print, audio or Braille.

*Calls to 03 numbers cost the same as calls to numbers starting with 01 and 02. Calls may be monitored or recorded for security and training purposes. Calls to 0800 numbers are free from landlines and mobiles. Charges for calls made outside of the UK will be determined by your local provider. Calls may be monitored or recorded for security and training purposes.

Information correct as at 11/2023

LSB
THE CONTINGENT REIMBURSEMENT MODEL CODE
APP SCAMS