transact

Q4 2026



Fraudulent contact and scam awareness

As we enter the final quarter, it is a good time to consider how we interact with our money, accounts and information, and the opportunities this can create for criminals. From answering an unexpected phone call to responding to a message online, everyday actions can sometimes provide criminals with an opportunity to target you.

This edition also highlights the growing use of spoofed phone numbers, where criminals make calls that appear to come from trusted organisations. Phishing scams remain one of the most effective methods used by criminals to steal information, gain access to bank and investment accounts, and cause financial harm. Alongside these risks, deepfake scams and Authorised Push Payment (APP) fraud continue to pose significant threats.

This leaflet highlights the latest fraud risks, explains how these scams operate, and outlines practical steps you can take to recognise warning signs and help protect yourself from financial loss and identity theft.

In order to reduce the risk of being a victim of fraud, here are some key tips which we strongly encourage for your general online use:

- Where possible, enable **Multi Factor Authentication**. We strongly suggest using an **authenticator app** (like Google Authenticator or Microsoft Authenticator), as it generates time-sensitive codes for added security. A guide on setting up MFA is available on our website and TOL.
- Avoid storing passwords on your devices in locations that are easy to access should your device be compromised – **use a password manager**.
- Use strong passwords with at least 12 characters, combining uppercase and lowercase letters, numbers, and special symbols (e.g. !, ?, #).
- **Pay attention to warnings from your bank** – The Confirmation of Payee service is designed to make sure you're sending the payment to the right person or business.

Deepfake scams

Deepfake scams use artificial intelligence to create convincing fake audio, video, or images that appear to show a real person.



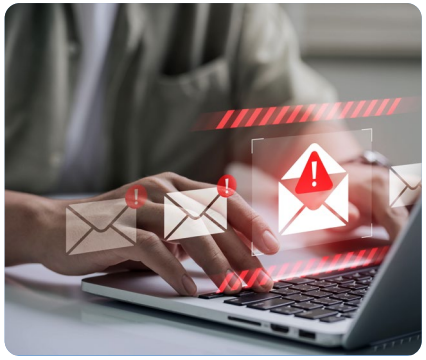
Deepfake scams use artificial intelligence to create convincing fake audio, video, or images that appear to show a real person. Recent Which? research found that 70% of UK adults tested could not correctly identify all of the real and AI-generated videos they were shown, highlighting how difficult convincing deepfakes can be to spot.

Criminals can clone a trusted voice or manipulate video footage to make it appear as though a family member, colleague, or public figure is urgently requesting money or sensitive information. They can use details gathered from social media or data breaches to make their approach more convincing. You may receive a voicemail that sounds like someone you know, or join a video call where the person appears genuine.

If you receive an unexpected or urgent request, pause and verify it using a known, trusted contact method. Never rely solely on voice or video confirmation when money or sensitive information is involved. Consider agreeing a safe phrase with family or close friends to help confirm their identity.

Phishing scams

Phishing scams remain one of the most common and effective ways criminals steal information and money online.



Fraudsters use phishing scams to trick people into clicking malicious links or downloading harmful attachments. This can allow criminals to steal personal information, gain access to online accounts, and ultimately lead to financial loss or identity theft. A common tactic is sending short 'probing' emails, such as "are you available for a chat?", to make you lower your guard. Once you respond, the scammer may attempt to steal information, request money, or send malicious links to gain access to further accounts.

Criminals often impersonate trusted organisations such as banks, delivery companies, or government bodies through convincing emails, text messages, or fake websites that appear genuine. These messages typically create urgency, claiming there is an issue with your account, a missed delivery, or suspicious activity that requires immediate action. To protect yourself, avoid clicking unexpected links or attachments and verify unusual requests through a trusted contact method.

Spoofed phone numbers

According to Report Fraud, there has been a rise in scam calls using 'spoofed' phone numbers. Criminals use technology to hide their real number and make calls appear to come from trusted organisations, such as your bank, the police or a government body.



A spoofed number can look genuine on your phone, making it easier for criminals to gain your trust. They may claim there is suspicious activity on your account or that you need to assist with an investigation, before asking for personal information, money or other sensitive details. Report Fraud warns that these calls can be automated or made by a real person.

If you receive an unexpected call, do not rely on the number displayed to confirm who is calling. Take your time, hang up and contact the organisation using a trusted number from its official website. Never share sensitive information or make payments simply because the caller appears genuine.

Authorised Push Payment (APP) fraud

APP fraud occurs when criminals deceive you into authorising a payment to an account they control.



Fraudsters use social engineering techniques to gather personal information from sources such as social media, phishing attacks, and data breaches. This enables them to create highly convincing communications, including calls, emails, texts, or deepfakes that appear genuine. These scams are designed to create urgency and pressure you into acting quickly.

Anyone can be targeted by APP fraud, but those who are less familiar with financial transactions online, or who are under emotional or financial stress, are at greater risk. Always verify payment requests independently and treat unexpected or unusual contact with caution.

Services and information

If you are contacted by someone claiming to be from your bank, stop, hang up and **dial 159**: the hotline designed to fight fraud. When you call 159, you'll get through to your bank directly and securely.

If you believe you've been targeted by scammers, report it to Report Fraud (previously Action Fraud) on **0300 123 2040** or at ***www.reportfraud.police.uk***, where you can also find more information on scams. If you're in Scotland, please report it to Police Scotland directly by calling 101.

Get more tips at ***www.takefive-stopfraud.org.uk*** and ***http://bit.ly/4i0ogxJ***

Sending money to Transact

Please avoid sending cheques or bankers drafts because they can be intercepted in the post on their way to us. The safest ways to make deposits into your Transact portfolio are through Transact Online (TOL: ***www.transact-online.co.uk***), using an active **direct debit** linked to the wrapper you wish to make the deposit into, or via **bank transfer**.

If you wish to send money via bank transfer

Our bank details are below:

Account Name: Transact Client Account

Name of Bank: NatWest

Account Number: 36298921

Sort Code: 60-00-01

You will need to use your **9-digit Portfolio Number** as the payment reference, so we can match the deposit to your portfolio. Please inform us that you have sent a deposit by logging into TOL, go to ***Transactions > Deposit*** or ***Deposit Then Buy*** pages and then follow the steps. That way we can allocate the deposit to the wrapper of your choice automatically and execute any investment purchases you have requested upon receipt of the deposit.

To make a deposit by Direct Debit

Log into TOL and go to ***Transactions > Deposit*** and select the **'Direct Debit'** option. Remember to select the wrapper you are making the deposit into.

If you have any concerns about your portfolio or feel the content in this guidance relates to you, then please contact your adviser or your Client Service team who will be able to help.

M291 (17) September 2026

"Transact" is operated by Integrated Financial Arrangements Ltd, 4th Floor, 2 Gresham Street, London EC2V 7AD | Tel: (020) 7608 4900 | Email: info@transact-online.co.uk | Web: *www.transact-online.co.uk* | Registered office: as above; Registered in England and Wales under number: 03727592. Authorised and regulated by the Financial Conduct Authority (entered on the Financial Services Register under number: 190856).