transact

Q3 2026

Fraudulent contact and scam awareness

As we move into the third quarter of the year, online activity continues to play a central role in everyday life, from managing finances and shopping online to communicating through digital platforms. As these habits become more routine, criminals continue to adapt their tactics to take advantage of them.

Phishing scams are on the rise and continue to be one of the most effective ways criminals steal information, gain access to bank and investment accounts, and cause financial harm. Alongside phishing, ongoing threats such as deepfake scams, Authorised Push Payment (APP) fraud, and SIM swap scams continue to evolve and affect individuals.

This leaflet highlights both emerging and persistent 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.

Key tips

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

- 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.

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.

SIM swap fraud

SIM swap fraud occurs when a fraudster takes control of your mobile phone number by transferring it to a new SIM card, allowing them to intercept calls, texts, and security codes to access your accounts.

According to Credit Industry Fraud Avoidance System (CIFAS), unauthorised SIM swap fraud has increased significantly in recent years, driven by the growing availability of stolen personal data and the use of more automated methods to compromise accounts. Once a fraudster gains control of your phone number, they can intercept calls and text messages, including security codes, enabling them to reset passwords, access your email and banking accounts, and steal funds before you realise.

If you suddenly lose service or suspect your SIM has been taken over, contact your mobile provider immediately and alert your bank so they can monitor for suspicious activity.

To protect yourself, add extra security to your mobile account by setting a PIN for SIM changes, use authentication methods that don't depend on SMS, such as an authenticator app, and stay alert for unexpected changes to your mobile service so you can act quickly if anything seems unusual.

Deepfake scams

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

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. These approaches draw on details gathered from social media or data breaches to increase credibility. You may receive a voicemail that sounds exactly like someone you know, or join a video call where the person appears genuine, with the aim of pressuring you into making a payment, sharing account details, or bypassing normal security checks.

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. One of the best ways to protect yourself is to come up with a safe phrase to check whether the call from your 'loved one' is real or not. It can become a sort of emergency code that only you and your immediate family or very close friends know, a simple and effective barrier against fraud.

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 (16) June 2026