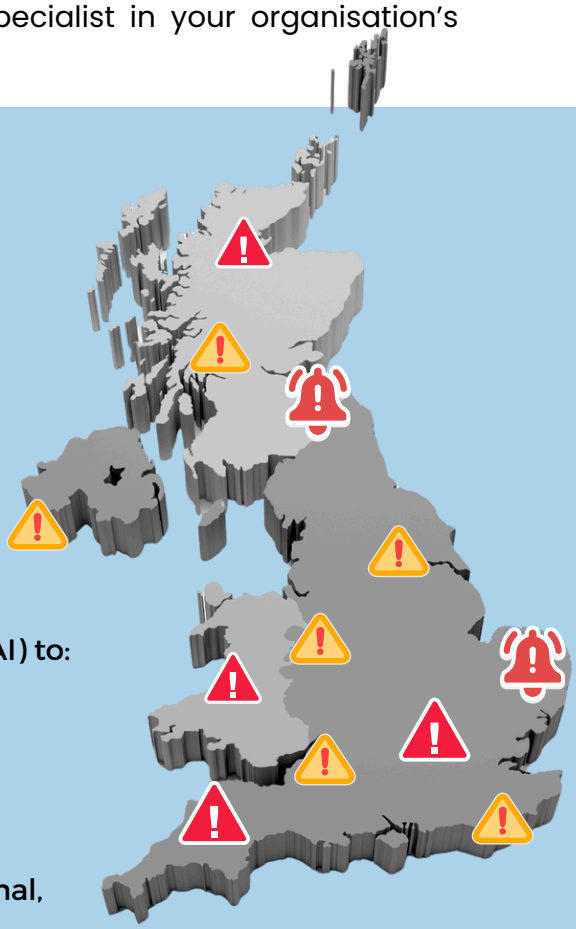
AUDIT YORKSHIRE

May 2026

Counter Fraud Newsletter

Welcome to this month's edition of the Counter Fraud Newsletter for NHS staff. You will find contact details for your Local Counter Fraud Specialist in your organisation's Anti-Fraud, Bribery and Corruption Policy.



UK Fraud Hits Record High

Fraud across the UK has reached record levels, with over 444,000 cases reported in 2025 – a 6% increase on the previous year.

This equates to more than 1,200 fraud incidents every day, highlighting the scale of the threat.

What's driving the increase?

Criminals are increasingly using artificial intelligence (AI) to:

- Create convincing fake identities and documents
- Carry out more sophisticated phishing attacks
- Automate fraud attempts at scale

Fraud is also becoming more organised and international, making it harder to detect and prevent.

Key trends to be aware of

- Identity fraud remains the biggest risk, accounting for over half of all cases.
- Account takeover continues to rise, particularly in mobile phones and online services.
- SIM swap fraud has increased significantly, enabling criminals to access accounts and bypass security checks.
- Money mule activity is growing, with individuals recruited via social media and job scams.

You can read more about the latest figures by visiting the CIFAS website:

https://www.cifas.org.uk/newsroom/fraudscape2026

If you think you have been the victim of fraud, you can report it to Report Fraud (the new name for Action Fraud) - you'll find details of how to do this on Page 4 of the newsletter.

Scam Focus : Sim Swap Fraud

As highlighted in the previous article, SIM-swap fraud is a growing risk, but what exactly is it, and how does it work?

SIM-swap fraud is a scam where criminals trick mobile phone providers into transferring your phone number to a SIM card they control.

Once this happens, they can receive your calls and texts – including one-time passcodes used to access bank accounts, email and online services.

Fraud prevention experts report a sharp rise in these attacks, driven by heavy reliance on text message security codes. In real cases, victims have lost thousands of pounds and faced weeks of stress while trying to regain control of their accounts and phone numbers.

Fraudsters usually start by gathering personal information about you – often from phishing emails, data breaches or social media.

They then contact your mobile provider, increasingly through online chat services, and pretend to be you. They may claim they've lost their phone or forgotten passwords. In some cases, repeated failed security checks were still followed by successful SIM swaps.

Once the transfer is approved, the fraudster moves quickly to reset passwords and intercept security codes.

How to Protect Yourself

- Be cautious of unexpected calls, emails or texts asking for personal or financial information
- Secure your mobile account with a strong password and any extra security your provider offers, such as a PIN
- Protect your email and online accounts with two-factor authentication (avoid SMS-based options where possible)
- Limit personal information shared on social media
- Act immediately if you receive an unexpected SIM-swap message or lose network service – contact your mobile provider and bank straight away

Your phone number is a key to your digital life. Taking these steps can significantly reduce the risk of SIM-swap fraud.

Conflicts of Interest Reminder

What is a conflict of interest?

A conflict of interest is anything that could reasonably be seen as influencing your NHS work—whether or not it actually does.

It could be financial (for example, links to a company) or non-financial (for example, a personal connection).

Conflicts can be actual, potential or perceived, which is why being open early really helps.

What should I declare?

If you're unsure whether something counts, the safest option is to declare it. Common examples include:

- **Outside work/roles:** paid or unpaid roles (including consultancy, directorships and private practice) that relate to your NHS duties.
- **Financial interests:** shares, ownership or other financial links with suppliers, providers or organisations you could affect through your work.
- **Gifts and hospitality:** offers or acceptance, in line with local policy (and record offers where your policy asks you to).
- **Close relationships:** friends, family or associates whose roles or interests could benefit from a decision you're involved in.

As a rule of thumb: declare when you start a role (and at any required annual review), whenever something changes, and before or during any meeting/decision where it might be relevant.

How to Declare

- **Find the policy:** look up your organisation's Conflicts of Interest / Standards of Business Conduct policy.
- **Record it and keep it current**: use your local declaration process (for example, ESR, a declaration portal or a form) and update it when things change.
- **Flag it early:** tell your line manager or meeting chair if you're unsure, or if you're involved in decisions such as procurement, commissioning, recruitment, research or supplier contact.

Take 5 minutes to check your declaration and update anything that's changed.

If you're not sure what to declare, speak to your line manager, meeting chair, or your organisation's corporate governance team (or equivalent).

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please notify your Local Counter Fraud Specialist. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.

You can also report your concerns to the NHS Counter Fraud Authority using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the Counter Fraud Team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Report Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.