AUDIT YORKSHIRE

August 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.

Reference Houses – What You Need to Know

Recruitment fraud remains an emerging risk across the NHS, and one of the methods increasingly being identified is the use of "reference houses" (sometimes referred to as "reference farms").

A reference house is a fraudulent set-up used during the recruitment process, where applicants pay an individual or illegitimate company to provide fake employment references.

These organisations often present themselves as small employers but may actually function more like unofficial recruitment agencies. In some cases, recruitment teams may see clusters of applicants using the same referee details for a company that cannot be verified.

The use of false references is not only dishonest, it can pose significant risks to patient safety and data security. Individuals using reference houses may be unqualified, unsuitable for the role, or concealing important aspects of their background.

Warning signs to look out for:

- Referees using personal email accounts rather than organisational addresses.
- Companies with little or no online presence.
- Use of residential or shared office addresses.
- Mobile-only contact numbers that are difficult to verify.
- References that are very quick, overly positive, vague, or identical.
- Employment dates or details that don't match the application.

These warning signs should prompt further checks and verification before progressing an application.

If you have concerns about a reference:

- Do not rely on the reference alone – seek independent verification.
- Contact the organisation directly using verified contact details.
- Discuss concerns with your Recruitment Team and/or Local Counter Fraud Specialist.

Early identification helps prevent unsuitable individuals from entering the organisation and protects both patients and staff.

NHS Fraud Case Highlights Importance of Speaking Up

A recent NHS Counter Fraud Authority (NHSCFA) investigation has led to the conviction of three individuals involved in a fraud that cost the NHS almost £280,000.

The case involved a former NHS employee who stole medical supplies from hospital stock rooms and arranged for them to be sold back to the same NHS trust through an external company. The fraud continued over several years before concerns about pricing and product identification numbers led to the scheme being uncovered.

The investigation also identified the movement of NHS funds through company and personal bank accounts linked to those involved. In addition to the financial losses, some of the medical supplies were found to be unsuitable for use, creating potential risks to patient care.

NEWS You can read the BBC news article about the case here

Why This Matters

Fraud against the NHS is not a victimless crime. Every pound lost to fraud is money that cannot be spent on patient care, staff, equipment and services. Cases such as this can also damage public confidence in the NHS and undermine trust in the people and systems that support healthcare delivery.

This case also demonstrates that fraud can sometimes be committed by individuals who have legitimate access to NHS premises, stock or systems. While the vast majority of NHS staff act with honesty and integrity, it is important that organisations maintain effective controls and that staff remain vigilant.

Spotting the Warning Signs

Fraud can take many forms, but common warning signs may include:

- Unusual purchasing patterns or pricing.
- Suppliers offering products at significantly lower prices than competitors.
- Stock discrepancies or unexplained losses.
- Concerns about the quality, origin, or condition of goods received.
- Transactions involving unfamiliar companies or suppliers.
- Individuals appearing to bypass established procedures or controls.

If Something Doesn't Feel Right, Report It

NHS staff are often best placed to identify concerns before significant losses occur. If you notice anything that appears suspicious, unusual, or inconsistent with normal processes, report it to the Counter Fraud Team. **Details are at the end of this newsletter.**

Raising a concern does not mean accusing someone of wrongdoing. It allows an impartial review of the information to determine whether further investigation is required.

By remaining alert and reporting concerns promptly, staff play a vital role in protecting NHS resources and ensuring that funding is used for its intended purpose – delivering safe and effective patient care.

Scam Index and Top Ten Frauds in the UK first quarter of 2026

More than 18 million adults in the UK have been targeted by scammers in just three months, new data from Virgin Media O2's first Scam Index reveals. The figures, published as part of a new quarterly snapshot revealing the fraud threat facing the country, come as official data shows fraud cases in England and Wales have risen 30% since 2017. Read their full article here.

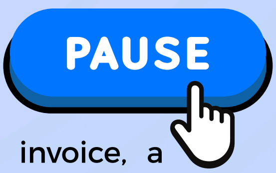
Top 10 scams seen in April to June 2026

1. **Delivery Scams:** Fake Royal Mail / DPD / Evri texts about held parcels, redelivery fees, or tracking updates.
2. **Online Shopping Scams:** Messages about an order you haven't placed or fake websites where paid-for items never arrive.
3. **Account Suspension Scams**: Claims your Apple, Microsoft, PayPal, Netflix, Amazon, or social media account will be locked unless you verify details.
4. **Banking / Finance Scams:** Fake messages claiming to be from your bank or payment provider about suspicious activity or account verification.
5. **Tech Support Scams:** Messages or calls claiming your device is infected or account compromised, urging you to call support or install software.
6. **Prize / Lottery scams:** "You've won!" messages for competitions you never entered, often requesting fees or personal information.
7. **Government / HMRC scams:** Fake tax refunds, grants, fines, National Insurance problems, or legal threats claiming to be from HMRC or other government departments.
8. **Telecoms Scams:** Fake alerts from O2, EE, Vodafone, etc., about bill issues, SIM swaps, or upgrades.
9. **Friends / Family Impersonation Scams:** Fake profiles, mobile numbers or hacked accounts pretending to be family, friends, colleagues, or verified accounts requesting money or codes.
10. **Investment / Crypto Scams:** Get-rich-quick schemes, fake trading platforms, crypto doubling, or bogus celebrity endorsements.

You can report messages by forwarding them to 7726 or text 7726 with the suspicious number.

7726

This is a free service available to customers on every UK mobile network.



Pause for Thought

Fraudsters count on people being busy. An unexpected invoice, a request to change bank details, or an email marked urgent can slip through when we're focused on getting things done. Taking just 30 seconds to pause, question, and verify can prevent a costly mistake. When it comes to protecting NHS resources, a moment of caution can make a big difference.

REPORTING FRAUD CONCERNS

Fraud against 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.