AUDIT YORKSHIRE

April 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.

Help Us Keep Track: Protecting NHS Equipment and Saving Money

Every day across the NHS, clinical and non-clinical teams rely on vital medical equipment to deliver safe, effective patient care. From monitors and pumps to specialist devices, this equipment is essential and it represents a significant investment for the NHS.

When equipment leaves our facilities with a patient, there is a real risk it may not return. Even a small number of missing items can quickly add up, leading to unnecessary replacement costs and reduced availability for other patients who need them.

We have also known of patients committing fraud by selling our valuable assets on, making a profit for themselves as well as a loss to the NHS.

Replacing missing equipment is expensive and avoidable. Every pound spent replacing lost items is money that could otherwise be used to support frontline services, improve patient care, or invest in staff and facilities. Keeping track of equipment isn't just an operational issue—it's a collective responsibility that directly supports the sustainability of our NHS.

What You Can Do
If equipment needs to leave a facility with a patient, please take a moment to help us keep accurate records:

- Let the Equipment Team know whenever equipment is issued to a patient for use outside of NHS premises.
- Ensure details are recorded clearly, including what item has been taken and, where possible, expected return arrangements.
- Encourage patients and carers to understand that the equipment remains NHS property and should be returned as agreed.
- Report concerns early if you believe equipment may be at risk of going missing.

If your department loans equipment to patients, please make sure that you know the contact details of your organisation's Equipment Team so that you can keep them updated and check what local procedures are in place.

Protect Yourself from Scams: Know When to Dial 159

In an article in last month's Counter Fraud Newsletter, we made reference to dialling 159, so let's go into more detail.

In an age where fraudsters are becoming increasingly sophisticated, it's more important than ever to know how to protect yourself and your finances. One of the simplest and most effective tools available to UK bank customers is the 159 phone service, a national anti-fraud helpline designed to connect you safely and directly to your bank.

What Is 159?

Launched in 2021 by Stop Scams UK, the 159 service acts as a secure shortcut to your bank's fraud team. Much like dialling 101 for the police or 111 for NHS advice, 159 is a trusted number that cannot be spoofed or impersonated. If you receive a suspicious call claiming to be from your bank, hang up. Wait for 15 minutes in case the fraudster has jammed your phone, or use a different phone, then dial 159. You'll be asked to name your bank and then you'll be connected directly to its customer service department.

When Should You dial 159?

- You receive a call asking for personal or financial information.
- You're told to transfer money urgently.
- You're unsure whether a call from your bank is genuine.
- You have entered your bank details into a suspicious link (we showed you how we used this in reality in our feature on Winter Fuel Payments Scams in our August 2025 newsletter).

Even if the call seems legitimate, it's safer to hang up and call back using 159. This breaks the scammer's contact and ensures you're speaking to your real bank.

The service currently connects to over 99% of UK retail banks and calls are charged at the same rate as a national call.

After calling 159, you will be asked which bank you would like to be connected to. You may then be asked to state why you are calling. From our own experiences, we suggest you say "fraud" if you've noticed unusual transactions, or "account security breach" if you've shared details but haven't seen any debits yet.

Spread the Word

The more people know about **159**, the fewer will fall victim to scams.

Please share this information with colleagues, friends, and family—especially those who may be more vulnerable to fraud.

Knock Knock... Who's There? It Could Be a Scammer

Doorstep scams are more common than you might think. In fact, recent research by home security company Ring found that nearly 1 in 5 adults were targeted in the past year alone.

These scammers are convincing. They often pretend to be from trusted organisations like energy companies, security services, or well-known brands, all to gain your trust and your money.

So, how do they do it?

Fraudsters rely on pressure and clever tactics to catch people off guard. For example:

- They might say they were "working nearby" and noticed an issue with your home—conveniently offering to fix it using "leftover materials".
- Some claim to have inspected areas you can't easily access, like your roof or loft, and show photos or videos as "proof" of urgent damage (which may not even be your property).
- Others go as far as staging problems—like creating the appearance of damp—to make the issue seem real.
- A big red flag is pressure to pay immediately, often in cash, or requests for a deposit on the spot. In some cases, they'll even offer to take you to the bank. Once you pay, they may keep finding new "problems" that need more money.

Of course, not everyone who knocks on your door has bad intentions. Utility workers, council officials, and charity representatives may call legitimately. The key is to always check before you trust.

How to protect yourself

- Always ask for ID—and don't be afraid to double-check it.
- If you're unsure, keep the door closed and contact the organisation directly using a trusted number.
- Never feel rushed into making a decision—genuine callers will not pressure you.
- Don't hand over cash or agree to work on the spot.
- If something doesn't feel right, say no.

If you've had a suspicious caller, you can also contact the Citizens Advice consumer helpline for advice.

For more tips on staying safe, take a look at Report Fraud, which provides practical advice on avoiding doorstep fraud.

If in doubt, keep them out. It's always okay to close the door and check first.

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.

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.