AUDIT YORKSHIRE

March 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 on the last page.

New Tools Helping to Tackle Scam Calls

Nationwide has introduced a new Call Checker tool to help people quickly verify whether a caller claiming to be from their bank is genuine.

According to research highlighted by Which?, the average person now receives around eight suspicious calls each month, with fraudsters frequently posing as trusted organisations to pressure victims into sharing personal details or moving money.

The Call Checker feature, accessed through Nationwide's mobile app, allows users to confirm instantly if they are speaking to a real Nationwide colleague or an impersonator.

Banks including Barclays, Monzo, Starling and Revolut are also adopting similar verification tools, giving customers more ways to challenge suspicious contact. For anyone unsure about a call from any bank, dialling 159 offers a quick route to official verification.

You can read the full Which? article for more detail on how these tools work and what other banks are doing to combat impersonation scams: Which? Article

DID YOU KNOW?

The "Spanish Prisoner" scam is over 400 years old, which involved fraudsters convincing victims to pay to "release" a wealthy prisoner in Spain — in return for a share of their fortune. It's basically the ancestor of today's advance-fee fraud.

Need to Contact Us?

Your Local Counter Fraud Specialist's contact details are on the last page.

GMC Impersonation Phishing Emails Targeting Doctors

We have received reports of phishing emails impersonating the General Medical Council (GMC) and targeting doctors.

These emails appear to come from the "General Medical Council" but originate from personal email accounts, such as a Gmail account.

Fraudsters claim to offer a three year GMC registration and licence to practise for £100. These messages use typical phishing tactics including false urgency, limited availability offers, and requests for personal information.

How to Spot This Fraud

Look out for emails that:

- Are sent from non GMC domains, especially free webmail accounts.
- Offer discounted or time limited GMC registration.
- Ask you to reply with personal details.
- Create pressure or urgency to respond quickly.

If You Receive a Suspicious Email

Do NOT:
❌ Respond to the email.
❌ Open attachments.
❌ Click any links.
❌ Provide any personal or professional information.

Do:
✅ Verify genuine GMC communications via the official website: www.gmc-uk.org
✅ Forward suspicious emails to spamreports@nhs.net (or your organisation's designated spam reporting mailbox).
✅ Delete the email from both your inbox and deleted items.

Former NHS HR manager ordered to repay almost £7k after lying about mother's death to defraud the NHS

A former NHS senior HR manager has been ordered to repay £6,948.25 after falsely claiming her mother had died so she could take time off from her role and work elsewhere.

Leanne Underhill, 46, received her sentence at Poole Magistrates' Court on Monday 16 February 2026. She was ordered to repay her full salary overpayment and the full investigation costs.

She had previously pleaded guilty to fraud by false representation at Poole Magistrates' Court on 4 December 2025.

She will make her repayments in monthly instalments of £150, starting from 1 March 2026. Underhill had been employed as a senior HR manager by University Hospitals Dorset NHS Foundation Trust. Read more here.

🚨 Watch Out for Fake NHS Cold Calls

GP surgeries and NHS organisations across the country are warning about a new wave of scam phone calls where fraudsters impersonate NHS services. These calls can appear convincing but they are designed to obtain personal information.

How the Scam Works

According to recent reporting by Which?, scammers are using automated messages to mimic NHS receptionists or doctors. These messages typically claim that your GP record is "out of date" and that you must update it urgently or risk being removed from the practice list. [which.co.uk]

Victims have reported being asked to **press 1** to "update details", after which the caller requests personal information such as:

- Name and address.
- NHS number.
- Date of birth.
- Other sensitive identifiers.

These calls often use **spoofed numbers**, making them appear genuine.

What the NHS Will Never Do

- It will never threaten to remove anyone from a patient list over the phone.
- It will never ask for financial information or bank details.
- It will never pressure you to update confidential information during an unexpected call.

If you receive an unexpected call that appears to be from the NHS:

📞 Hang up if something feels off.

🕰️ Wait 15 minutes to make sure the call has definitely disconnected – scammers can jam your phone line even when you think you have hung up.

📢 Contact the NHS service that was apparently calling using an official number — from the NHS website, appointment letter, or your GP practice's site.

If you believe you've received a scam call or shared information:

🏥 Speak to your GP practice to confirm your records are secure.

🪙 Notify your bank if you've disclosed financial details.

❗ Report the incident to Report Fraud.

You can read the full Which? article here.

Fraud Awareness : Free Sessions for All Staff

The Counter Fraud team offers friendly, informal fraud awareness training for all staff —no prior knowledge needed, just an interest in helping to protect NHS resources.

We're currently refreshing the programme and will publish an updated timetable from April 2026.

We offer a range of sessions. Some provide a broad overview of fraud risks in the NHS whilst others are role-specific—for example, tailored sessions for colleagues working in HR, Procurement, or Creditor Payments.

You'll learn how to spot the signs of fraud and what to do if you have concerns, plus practical tips to help you look after your own finances and protect NHS money.

Sessions last around one hour, are delivered via Microsoft Teams, and are free to attend —just check that your line manager is happy for you to join.

Want the new timetable as soon as it's published? Email us at yhs-tr.audityorkshire@nhs.net and we'll send the details when it's released.

In the meantime, the Counter Fraud team can also attend your team meeting to share practical advice, deliver a focused session on a key fraud risk area, or support you with fraud prevention queries.

To arrange a visit, please use the contact details on the last page or email us at yhs-tr.audityorkshire@nhs.net

If there's a fraud topic you'd like us to cover in future sessions, please let us know—we welcome your ideas and suggestions.

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 on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

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 Counter Fraud Team will be happy to advise.

Our contact details are on the next page.

CONTACT US

Acronym Decoder
LCFS - Local Counter Fraud Specialist
LSMS - Local Security Management Specialist
ICB - Integrated Care Board

Steve Moss
Steven.Moss@nhs.net / 07717 356 707

Head of Anti Crime Services / LCFS

Steve manages the Counter Fraud Team.

Marie Dennis
Marie.Dennis2@nhs.net / 07970 265 017

Assistant Anti Crime Manager covering all clients, and LCFS covering:

FCMS

York and Scarborough Teaching Hospitals NHS Foundation Trust

Nikki Cooper
Nikki.Cooper1@nhs.net / 07872 988 939

LCFS Covering:
Humber Teaching NHS Foundation Trust

Humber and North Yorkshire ICB

Leeds Community Healthcare NHS Trust

Rosie Dickinson
rosie.dickinson1@nhs.net / 07825 228 175

LCFS Covering:
Harrogate and District NHS Foundation Trust

Spectrum Community Health CIC

West Yorkshire ICB

Shaun Fleming
ShaunFleming@nhs.net / 07484 243 063

LCFS and LSMS Covering:

Calderdale and Huddersfield NHS Foundation Trust

West Yorkshire ICB

Lincolnshire ICB

Rich Maw
R.Maw@nhs.net / 07971 846 865

LCFS Covering:

Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

Mid Yorkshire Teaching NHS Trust

Lee Swift
Lee.Swift1@nhs.net 07825 110 432

LCFS Covering:
Airedale NHS Foundation Trust

AGH Solutions

Bradford District Care NHS Foundation Trust

Leeds and York Partnership NHS Foundation Trust

NHS Professionals

You can also report fraud concerns to the NHS Counter Fraud Authority:
0800 028 40 60
https://cfa.nhs.uk/reportfraud

Follow us on X - search for @AYCounter Fraud

Visit our website or scan the QR code to read previous newsletters.