AUDIT YORKSHIRE

January 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.

PREDICTED NHS FRAUD TRENDS FOR 2026

Fraudsters are getting smarter, and the NHS is a target. Here's what to watch out for this year:

1. AI-Powered Scams
Criminals are using artificial intelligence to create fake voices and videos. A phone call or video might sound like a senior manager—but always verify requests for payments or sensitive data through official channels.

2. Synthetic Identities
Fraudsters mix real and fake details to create new identities. This can affect recruitment, patient records, and supplier onboarding. Look out for unusual documentation or inconsistencies.

3. Social Engineering
Scams are moving beyond email. Expect more fraud attempts via text messages, social media, and messaging apps. Never share login details or click suspicious links.

4. Instant Payment Risks
Faster payment systems mean fraudsters can move stolen funds quickly. NHS finance teams should double-check urgent payment requests.

What you can do

- Confirm all requests for payments or sensitive data through trusted channels.
- Report suspicious activity immediately to your Local Counter Fraud Specialist.
- Stay informed—fraud prevention is everyone's responsibility.
- If you have concerns, contact the NHS Counter Fraud Team. Our contact details are in your organisation's Anti-Fraud, Bribery and Corruption Policy.

Stop & Check: If something feels urgent or unusual, pause and verify.

Protect Your Access: Never share passwords or smartcard details.

Report Quickly: The sooner you report, the easier it is to stop fraud.

Scam Watch: Emails Impersonating Banks

Consumer affairs group Which? has recently warned about two convincing email scams impersonating banks. These scams aim to trick you into sharing personal details or downloading harmful software.

What's happening?
The emails claim you need to provide extra information or set up new security measures to recover or keep access to your account. This is a classic pressure tactic designed to make you act quickly without thinking.

How does the scam work?

- You're asked to click a link to "verify" your details to keep or recover access to your account.
- The link will take you to a phishing site, which can lead to criminals stealing your personal data or installing malware on your device.
- The emails use official logos and branding to look genuine.

These scam emails look professional, but there are warning signs to look out for:

- The emails don't come from official bank email addresses.
- Links within the message won't take you to the banks real website.

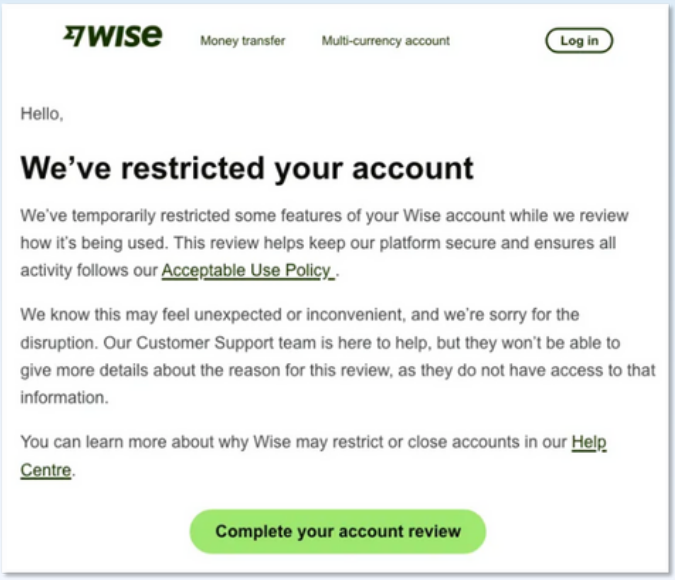
Please be aware that if you're checking emails on a mobile phone or tablet, these clues can be hard to spot.

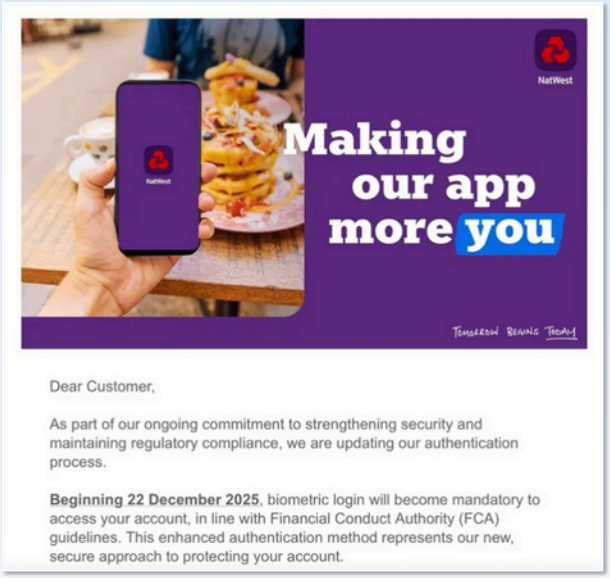
What should you do?

If you're unsure whether an email is genuine:

- Don't click any links.
- Call your bank directly using the number on the back of your card.
- Never trust phone numbers or links provided in suspicious emails.

You can find out more about scams doing the rounds on the Which? website.





Car Finance Compensation Scams – Don't Get Taken for a Ride

With headlines full of news about mis-sold car finance and potential payouts, fraudsters are jumping on the bandwagon to trick people into handing over personal and financial information. Here's what you need to know to stay safe.

The Financial Conduct Authority (FCA) has just finished a consultation on a redress scheme for people who were mis-sold car finance between 2007 and 2024. This includes cases where:

- You weren't told about hidden commissions paid to dealers.
- Your interest rate was inflated to boost a broker's earnings.
- You were misled about the terms of your finance agreement.

If the scheme goes ahead, you won't need to pay anyone to make a claim, you will be able to do it yourself for free. The official rules on how to claim are expected to be announced in early 2026.

The Scam: "You're Owed £3,000 – Just Confirm Your Bank Details"
Fraudsters are cold-calling, texting, or emailing people claiming to be from:

- The FCA
- A law firm
- A car finance company

They say you're owed compensation and ask for your bank details, National Insurance number, or even an upfront fee to "process your claim."

These are scams. The FCA has confirmed it is not contacting individuals directly and no payments are being made yet.

How to Protect Yourself

- Don't respond to unsolicited calls or texts about car finance claims.
- Never share personal or financial details unless you're 100% sure who you're dealing with.
- Check the FCA register to see if a company is authorised: https://www.fca.org.uk
- The Martin Lewis website has a free tool to help you make your own claim https://www.moneysavingexpert.com/reclaim/reclaim-car-finance/
- If you have been the victim of a car finance refund scam, notify Report Fraud: www.reportfraud.police.uk 0300 123 20 40

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 LCFS 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.