SEPTEMBER 2025

AUDIT YORKSHIRE

# COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud Newsletter. We hope you find the contents helpful. As always, if you need any fraud advice please reach out to your Local Counter Fraud Specialist. You'll find our details on the last page.

**Failure to Prevent Fraud - New Legislation**

New legislation came into force on 01/09/2025 which makes certain companies accountable if they do not take adequate steps to prevent fraud. Most NHS trusts and related entities will need to comply.

If a member of staff, or someone acting on behalf of the NHS, commits fraud for business gain, and the employer did not have reasonable procedures in place to stop it, the employer (i.e. the NHS organisation) can be prosecuted.

A strong defence is to show that "reasonable procedures" were in place. This usually means having clear policies, regular training, effective controls, and easy ways for staff to raise concerns.

Those found guilty can face heavy fines, reputational harm, and closer attention from regulators.

It is therefore essential that any suspicions of fraud are reported.

Every report made to your Local Counter Fraud Specialist, whether substantiated or not, helps identify weaknesses in existing processes, allowing us to strengthen our controls. It also creates a true reflection of the risk of fraud in the NHS.

By having a better understanding, the Counter Fraud Team will be able to put measures in place to prevent future frauds, put right any wrongs which have happened and build effective controls to comply with the new Failure to Prevent Fraud legislation.

Don't worry about whether or not the activity you are aware of is fraud according to the legislation. Please tell us anyway and if it needs to be looked at by somebody else, we'll help to arrange that.

All reports we receive are dealt with confidentially and we will work with you to decide the best way forward.

Please see your organisation's Anti-Fraud, Bribery and Corruption Policy and Whistle Blowing Policy for more information.

Please report any suspicions of fraud you receive. Details of how to do this are at the end of this newsletter.

## Amazon Gift Card Scam Targeting NHS Staff

### What does the scam look like?

We are aware of some instances where emails are being received in NHS organisations, starting with very vague requests, such as 'please can you confirm you have received this email'.

If they get a response, the email sender goes on to say that they are trying to buy an Amazon gift card for a friend's daughter who has been diagnosed with cancer, but they have not been able to complete the purchase.

It is believed that the purpose of this email is to try to persuade a member of staff to make the purchase on behalf of the email sender.

We have seen this email twice:

- One was pretending to be from a patient where the initial request was to discuss treatment.
- The second was allegedly from a member of staff. We believe that the member of staff who was impersonated was identified using LinkedIn, as the bio from the public facing profile was mirrored in the email signature.

### How can I avoid this scam?

Not all email requests are genuine, and it is important to approach them with caution. Cybercriminals often use emails to disguise malicious intent behind what appears to be a normal request.

These emails may impersonate trusted colleagues, companies, patients or services. They are designed to manipulate recipients into sharing sensitive information, clicking on harmful links, taking actions they would not normally do (in this case, make a purchase) and / or opening infected attachments.

Even seemingly harmless or routine requests can be crafted to build trust and lower defences, paving the way for more targeted attacks. By being aware of the risks and carefully verifying requests, we can help to protect ourselves and the NHS from potential security breaches.

We'd also like to remind staff about oversharing on social media as personal information can be used against you or to impersonate you. Keep your settings private where possible and be mindful of what you do post.

For more details about what to do if you receive a suspicious email, please see page 4 of this newsletter.

QUICK TIPS

## CHECKING SUSPICIOUS EMAILS AT WORK

- **Check the sender's address carefully** – look for subtle misspellings, unusual domains, or addresses that don't match the supposed sender.

- **Hover over links before clicking** – verify that the URL matches the expected destination and doesn't redirect to a suspicious or unrelated site.

- **Be cautious with unexpected attachments** - if unsure, do not open them.

- **Look out for urgent or unusual requests –** messages pressuring you to act quickly (e.g., "pay now," "update your password") are common phishing tactics.

- **If in doubt, get advice from your Local Counter Fraud Specialist or IT team.**

**Parking Fine Scam Text Messages**

A scam has been spotted where fraudsters send out text messages claiming that you owe money for an unpaid parking fine.

The text message contains a link to what appears to be an official GOV.UK website but is actually a phishing platform. The fraudsters have taken great care to use the correct logos and branding to make the site look real.

Typically, the message will include a **short deadline** and **threats** that the recipient will lose their driving license and face legal action if payment is not made. An example of the message content is shown on the right hand side of this page.

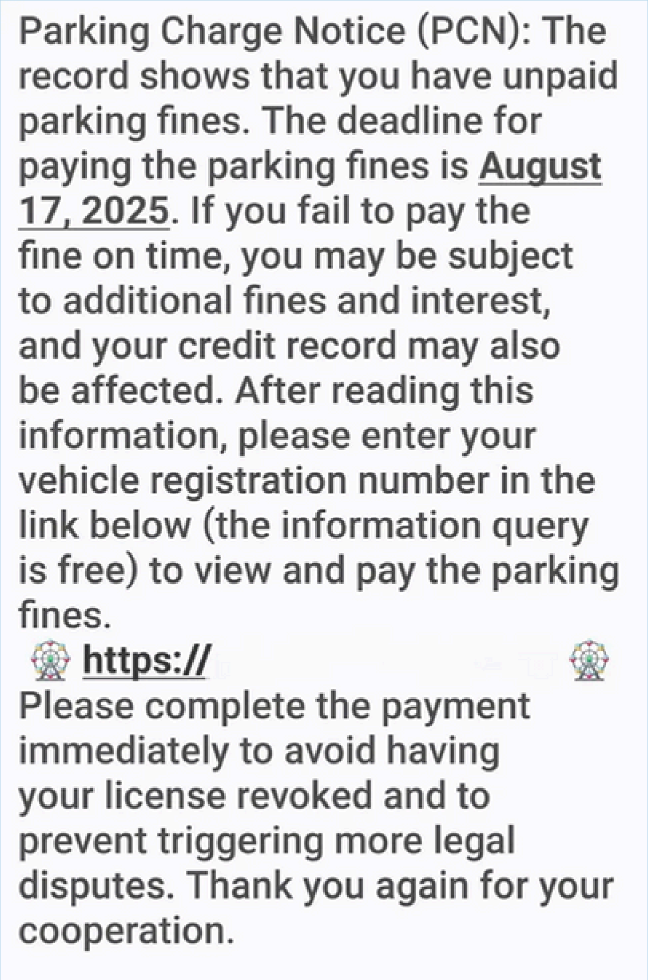
Which?, the consumer affairs company, has investigated this scam methodology. They have found that if you access the link, you are prompted to enter your vehicle registration number. Note that the text message doesn't contain your vehicle registration number – as the fraudsters don't know it yet!

Researchers at Which? entered a range of random characters into the vehicle registration field and every time the dodgy site claimed that a parking fine was due.

It also appeared that the website was accessing the person's location data and using that information to make it look as though the parking fine originated from the local area.

Once the researchers went onto the next page, they were invited to add personal and financial information.

You can read more about their investigation here: [Scam alert: new parking fine scam text - Which?]


Parking Charge Notice (PCN): The record shows that you have unpaid parking fines. The deadline for paying the parking fines is August 17, 2025. If you fail to pay the fine on time, you may be subject to additional fines and interest, and your credit record may also be affected. After reading this information, please enter your vehicle registration number in the link below (the information query is free) to view and pay the parking fines.
🎡 https:// 🎡
Please complete the payment immediately to avoid having your license revoked and to prevent triggering more legal disputes. Thank you again for your cooperation.

**Staying Safe from this Scam**

- If you receive an unexpected text message, don't click on links or enter personal details.
- If a parking fine is genuine, the organisation issuing the fine should provide your vehicle registration and details of the specific date / time / location of any parking violation.
- You can forward scam text messages to 7726.
- Remember, all official government websites start with GOV.UK.
- There is guidance on parking penalty charges on the GOV.UK website: https://www.gov.uk/parking-tickets

# 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 **Action 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.