OCTOBER 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.

Watch Out for Fleeceware

Not to be confused with **fleece-wear**. This type of scam is far from a cosy jumper you can snuggle into as the days get shorter and colder.

These are apps which can be downloaded onto mobiles, which literally fleece users into overpaying for features or functions. This could be by charging for something which can be found for free, or at a much cheaper cost.

Another tactic is to offer a trial period then demanding extortionate amounts after this has expired.

Which? has reported on a scam ParentPay app in Apple's App Store.

ParentPay is an online way that schools can collect money from parents. The genuine service is available online, but not as an app to be downloaded. The fake app redirected users elsewhere and charged a £40 a month subscription fee.

Whilst downloading apps from authorised stores, such as Google Play and the Apple App Store offers some protection, care must be taken. Dodgy apps can find their way into stores if they do not contain malware or do not breach the listing terms and conditions.

To avoid fleeceware:

- Be wary of adverts for apps on social media, especially the ones which seem too good to be true.
- Research apps and compare similar ones before downloading. Make sure you read all the small print.
- Make sure you know what you will be paying after a free trial ends. Also look out for very short free trials, some are less than a week.

You can check subscriptions you have by doing the following:
Apple - settings > tap your name > subscriptions
Android – open Play Store > tap lined menu option (top right of screen) > subscriptions

In the Press : Covid Vaccination Fraud

On 18th July 2025, a former NHS worker was sentenced to 24 months in prison after pleading guilty to fraud by false representation. Wayne Knight had conspired to create false Covid-19 vaccination records in exchange for payment.

Between July and November 2021, Wayne Knight, a Senior Healthcare Worker at a London Trust, assisted in creating 238 false records which claimed that a person had received a vaccination when they had not. His actions would have placed vulnerable members of society at risk.

You can read more about the case on the Crown Prosecution Service website:
Covid-19 Vaccination Conviction

Care Quality Commission (CQC) Impersonation scam

The CQC have had an increase in reports of people posing as CQC inspectors to gain access to personal information of staff and financial information of organisations at various care providers. This is now being investigated by the Police.

Some of the contacts have been made by phone call. Here's how it works: a call is received from a bogus inspector, asking to speak to a manager. The "inspector" may quote details of the previous CQC inspection report to make themselves sound legitimate. CQC reports are in the public domain, so this detail does not verify that the caller is genuine.

Then, or at a later time, a 'telephone inspection' occurs. The caller requests personal information and/or the organisation's financial information, bank account details etc. **A genuine CQC inspector will never ask for provider or personal bank account details over the phone as part of the inspection process.**

Guidance regarding what to do if you think that you have been approached in this way is on the CQC website here .

Genuine CQC Inspectors carry ID badges that include:

✅ A photograph of the inspector.
✅ A copy of the CQC warrant on the reverse.
✅ The signature of the CQC Chief Executive in post when the card was issued.

If you are contacted by phone or email:

📞 CQC inspectors will not ask for bank details or personal information about staff over the phone.
❓You can ask for requests for information to be made to you in writing.
📧 Emails should come from @cqc.org.uk accounts.
📌 You can offer to supply information by sending it to the CQC's main postal or email address.
🔍 Consider whether the person is asking for information that the CQC should already have (such as the name and ID of your registered manager).

If you are unsure about the identity of an inspector, please call the CQC on :
03000 61 61 61

Gift Card Draining Scam

West Yorkshire Police are warning of a new type of gift card scam. They have become aware of criminals tampering with gift cards in shops - taking note of the card number and PIN, then resealing the packaging.

They put the compromised card back on the shelf. If anyone adds credit to the gift card, the fraudster then redeems the value before it reaches the intended recipient.

West Yorkshire Police believe that gift cards are being stolen, tampered with, and then replaced in shops. To protect yourself from this scam, they recommend:

- Inspect cards for signs of tampering.
- Buy cards from secure displays or from behind the counter .
- Register your card online immediately, if possible.
- Avoid third-party sellers offering discounted cards.
- Never pay bills or fines with gift cards.

Fraud Risk Focus: Expenses Claims

Submitting expense claims is a normal part of NHS work — whether it's travel costs, training, or other approved expenses. Most claims are genuine and essential. But sometimes, mistakes or misunderstandings can lead to incorrect claims being submitted.

It is important we all take a few simple steps to make sure expense claims are accurate, fair, and in line with NHS policy. By doing so, we help protect NHS funds, maintain trust, and ensure resources are used where they're needed most — for patient care.

📝 **Common Pitfalls (Often Unintentional!)**

- Claiming for items not covered by your organisation's policy.
- Submitting the same receipt twice by mistake.
- Using estimates instead of actual costs.
- Forgetting to include receipts for proof of payment.
- Claiming mileage for journeys that weren't work-related.

📌 **Tips for Getting It Right**

✓ Keep receipts for all purchases and travel. Make sure you keep them organised so you know which ones have been submitted.
✓ When scanning in or photographing receipts, make sure you capture the entire document.
✓ Check the policy before submitting a claim - if in doubt, seek advice from your manager.
✓ Make sure your mileage and dates are accurate. It can be helpful to record journeys in your calendar or diary as you go along, to help you keep track.
✓ Ask your manager or payroll team if you're unsure about how to submit a claim or what you can claim for.
✓ Double-check claims before submitting to avoid duplicates.

🤝 **Why It Matters**

Every pound saved from incorrect claims helps fund vital services, staff, and patient care. By taking care with our expense claims, we're all playing a part in protecting NHS resources.

🚨 **If You Spot an Issue**

If you realise a mistake has been made on your claim, let your manager or payroll team know — errors can be corrected quickly.

If you suspect deliberate fraud, report it:

- Contact your Local Counter Fraud Specialist (LCFS)
- Or use the NHS Fraud & Corruption Reporting Line: 0800 028 4060

Thank you for helping us keep the NHS strong, fair, and supportive for everyone!

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.