



Fraud Counts Newsletter

International Fraud Awareness Week 2023 – Edition 1



Introduction

Welcome to our latest edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on how you can play a vital role in preventing fraud, current scam trends including the Cost of Living scam and Property to Rent scams, fraud cases currently in the press, a reminder on reporting fraud concerns, and how to contact your Local Counter Fraud Specialist.

Fighting Fraud Together

In today's digital world, fraud has become more advanced. Cyber-criminals are constantly creating new ways of trying to trick people. However, all of us can play a vital role in preventing fraud.

Education Is Your Shield

Staying informed about the latest scams is your first line of defence. The more you know about how fraudsters behave and what their current strategies are, the better your chances of spotting scams at home and at work.

Scepticism: Your Inner Lie Detector

When you encounter suspicious emails, adverts, text messages or other offers that seem too good to be true, being sceptical can save you from trouble. Always take the time to consider what steps you can take to check if something is legitimate. There is plenty of advice available online covering loads of different scam types (e.g. search "romance scam advice" or "Facebook marketplace scam advice" to see some examples).

Listen to Your Gut (Intuition)

If something feels off, take a moment to pause and think. This piece of advice is central to the fraud awareness campaign run by [Take 5 to Stop Fraud](#), as fraudsters will often try to panic you or rush you into making a mistake.

Speak Up and Report

Talking about fraud and reporting it can help prevent others from falling into the same traps. It also exposes the tactics fraudsters use. You'll find advice on how to report different types of fraud on page 3 of this newsletter.



In our interconnected world, people armed with knowledge, scepticism, intuition, and open communication are the front line of defence against fraud. **Together, we can outsmart the fraudsters and keep ourselves and others safe.**



Current Scam Trends

Cost of Living Scam

With the Government due to make further cost of living payments over the coming months, there is an increased risk that fraudsters will try and deceive you. They will do this by pretending to be the Department for Work and Pensions (DWP) and could target you by phone, email or text.

The fraudsters are unlikely to know who is eligible and may contact you even if you are not entitled to a payment.

One of the text messages which has been seen is:

“ GOV: The £750.00 (GBP) Living Payment is ready, take action by accepting the payment via legallaid.income-division.com ”

This link leads to genuine looking website which asks for your name, address and bank details.

Property to Rent Scams

Fraudsters have been taking advantage of the shortage of rental properties, rising rent prices, and high levels of demand. Usually, these scams start with a post on social media advertising a property or room to rent at an attractive rate.

In some of these scams, the fraudster asks the victim to pay a deposit or rent in advance even before the victim has been able to view the property. Once paid, the fraudster cuts all contact.

In other cases, victims have been shown around properties, asked to sign official-looking contracts, and have even been given keys after paying a deposit. However, when they later try to move in, they find their key doesn't work and/or that there is someone else already living at the address. The “landlord” vanishes, leaving the victim out of pocket.

Prevention Advice

DWP have warned that you need to be mindful if you receive any contact asking you to apply, accept or get in touch with somebody to receive the payment as this may be a scam.

- ⚠ If you are eligible, you do not need to apply to receive the payment. It is done automatically.
- ⚠ DWP will not ask you for personal details via text or email.
- ⚠ If you have entered your details on a site like this, contact your bank immediately. You can call 159 and the hotline will connect you to your bank.
- ⚠ Suspicious text messages can be forwarded to 7726 and dodgy emails can go to report@phishing.gov.uk

Prevention Advice

- ⚠ Be wary of accommodation advertised on social media or unregulated platforms. Photos can be stolen from genuine listings.
- ⚠ All letting agents and property managers must be registered with a government-approved redress scheme. [The National Trading Standards website](https://www.which.co.uk/consumers/property/) has a tool where this can be checked.
- ⚠ Look out for pressure tactics - if the “landlord” is trying to panic you into sending money, take a step back. · There is more advice on how to keep yourself safe from these scams on the [Which? website](https://www.which.co.uk/consumers/property/).



In the Press



Prison Sentence following £560k NHS fraud

Thomas Elrick had been a senior manager at NHS Harrow Clinical Commissioning Group. His role gave him access to a budget and the ability to authorise payments worth up to £50,000.

Elrick abused this trusted position in order to pay invoices which added up to over £560k to a company which had not provided any services to the CCG. The company was a dormant business, and in fact, Elrick was sending the payments to his own bank account.

To try and cover up the fraud, Elrick used an email account of his deceased wife to send emails to the CCG. He even created false details regarding services he claimed had been provided by the dormant company.

Elrick had spent the money on expensive holidays and shopping. In interview he admitted the offences and has been sentenced to 3 years and 8 months in prison. You can read more on the [NHS Counter Fraud Authority website](#).

Keeping yourself safe

Always be suspicious if you are asked to click on a link in an email or on a social media post.



If you are on a desktop or laptop, you can use your mouse to hover over the link to see where it will take you.



It is not easy to hover over links on touch screen devices. If in doubt, log into a desktop/laptop and hover over the link.



Be wary about which apps you download – you can find some useful advice on safe app interaction on the Verified website.

Suspensions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence - 0800 028 40 60 or www.reportnhsfraud.nhs.uk





A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS.	You can contact your local Counter Fraud team using the details overleaf. You can also report your concerns to the NHS Counter Fraud Authority, via their online reporting tool, or hotline. If you making an anonymous report, please give as much detail as possible, as we won't be able to contact you for more information.
I have a concern that fraud may be being committed against the general public.	These concerns can be reported to Action Fraud (0300 123 2040). If someone has been actively defrauded it may also be appropriate to report to the police. If it is suspected that the victim's bank account has been compromised, they will need to speak to their bank as a matter of urgency.
I have received a suspicious email to my NHS.net email address.	Do not click on any links or attachments. Forward the suspect email as an attachment to spamreports@nhs.net . To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".
I have received a suspicious email to another email account (not NHS.net).	Do not click on any links or attachments. Forward the email to report@phishing.gov.uk . You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.
I have received a suspicious text message.	Do not click on any links in the text message! Forward the text message to 7726.
I have come across something and I'm not sure whether or not it is fraud related.	You are very welcome to contact your local Counter Fraud team for advice and support using the details overleaf.

**Fraud in Your
NHS Workplace?**
Report it!



If you have any suspicions or concerns,
You can call us anonymously on

0800 028 40 60

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information
The NHS Counter Fraud Authority leads on fighting fraud, bribery
and corruption in the NHS and the wider health group


Counter Fraud Authority


Department
of Health &
Social Care



Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact one of our team below.



Gareth Cottrell – Counter Fraud Manager

✉ gareth.cottrell@nhs.net ☎ 01872 258057
07814 002364



Tracy Wheeler – LCFS

✉ tracy.wheeler2@nhs.net ☎ 01752 431378
07789 868568



Byron Kevern – LCFS

✉ byron.kevern@nhs.net ☎ 07775 417508



Sarah Smith – LCFS

✉ Sarah.Smith10@uhbw.nhs.uk ☎ 07467 685609



Sandra Bell – LCFS

✉ sandra.bell19@nhs.net ☎ 07467 685529



Ian Halkerd – LCFS

✉ ian.halkerd@uhbw.nhs.net ☎ 07788 300215



Sammy Donaldson – Trainee LCFS

✉ s.donaldson1@nhs.net ☎ 07467 685529