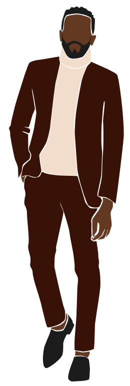
AUDIT YORKSHIRE

July 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.



Behind the Dream: Spotting Fake Modelling Agencies

Think you've found your big break?
Scammers prey on aspiring models with promises of fame and fortune, only to leave them out of pocket and disillusioned.

This used to be something which affected younger people, but fraudsters are now targeting older generations by claiming there is a shortage of mature models.

How These Scams Work

Fraudulent agencies often:

- **Charge Upfront Fees** for registration, guaranteed jobs, or portfolio shoots.
- **Create Urgency:** "Sign today or lose your chance!"
- **Promise Guaranteed Success** —no agency can guarantee work.
- **Push Overpriced Photo Packages** with in-house photographers.
- **Use Unprofessional Communication.** Poor grammar, generic greetings, or free email domains.

Also be wary of:

- Requests for nude or suggestive photos.
- Vague contracts or refusal to allow review time.
- Contact via social media DMs with unrealistic promises.
- Pressure to pay immediately.

Stay Safe: Practical Tips

1. **Research Before You Sign:** Check reviews and verify credentials.
2. **Never Pay Upfront:** Legitimate agencies earn through commission.
3. **Verify Casting Calls:** Contact brands directly.
4. **Protect Your Personal Info:** Never share bank details early.
5. **Trust Your Instincts:** If it feels wrong, walk away.

If You've Been Targeted

- Stop all communication immediately.
- Report the scam to [Report Fraud.]
- Share your experience to warn others.

Think before you sign.

Understanding Virtual Credit Cards:
Benefits, Risks, and Why Controls Matter

Virtual Credit Cards (VCCs) are becoming increasingly common across the NHS as organisations look for safer, more flexible ways to manage business-related spending.

Recent guidance from the NHS Counter Fraud Authority (NHSCFA) highlights both the advantages of VCCs and the risks that can arise without proper oversight. Here's what you need to know.

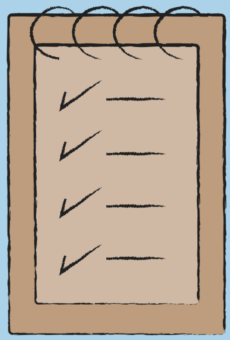
What is a VCC?

A VCC is a temporary, digital version of a traditional credit card. Instead of a physical card, a bank or card issuer generates a unique card number, expiry date and CVV code which can be used for transactions. These digital cards can be stored on mobile pay apps or digital wallets, meaning they are not restricted to online purchases.

Not all banks offer VCCs, and some use different terminology. For example, NatWest refers to its product as Virtual Pay, while HSBC provides Virtual Card Solutions for business customers. In some cases, third-party providers support the service.

Key Benefits of VCC

VCCs offer several security and operational advantages, including:



- **Enhanced fraud protection:** VCCs act as a 'mask' for the real card details, reducing the risk of card data being stored or misused.
- **One-time usage options**: If card details are compromised, they cannot be used again after the initial purchase.
- **Digital-only convenience:** Because VCCs are created and controlled through banking apps, new card details can be generated quickly and even tailored for specific merchants.
- **Easy to freeze or cancel:** As they are digital, VCCs can be stopped instantly if suspicious activity is detected.

Understanding the Risks

Despite their benefits, VCCs are not risk-free. The NHSCFA has identified vulnerabilities where organisations have assumed virtual cards require less scrutiny than physical ones. Therefore there needs to be the same levels of oversight to VCCs as to physical ones.

As VCC usage expands, it brings significant security benefits but also new opportunities for fraud if not properly managed. Ensuring consistent oversight, clear policies, and strong internal controls will help NHS organisations safeguard public funds and maintain confidence in digital financial tools.

If you have any concerns about VCCs and would like any further information or advice, please contact your Local Counter Fraud Specialist.

Ghost Brokers- Fake Car Insurance Targeting Young Adults

Young drivers are being targeted by "ghost brokers" selling fake car insurance online, the Financial Conduct Authority (FCA) has warned.

Half of drivers aged 16-25 have bought policies through social media or messaging apps, many of which are fake, research from the FCA suggested.

Some victims are unknowingly driving without insurance, meaning they could be prosecuted, fined or have their car seized, the FCA said.

Often the "policies" are suspiciously cheap, but many young drivers stretched by cost of living pressures are lured in.

Driving without valid insurance is a criminal offence in the UK.

The Insurance Fraud Bureau (IFB) and insurance company Aviva have both reported an increase in ghost broking in recent years.

The FCA Firm Checker can be used to confirm a broker is authorised. FCA advice is that legitimate insurance brokers should have a website, phone number and address.

The FCA surveyed 1,000 drivers and found that many ghost brokers pose as legitimate insurance sellers but offer cheap rates.

The policies are often completely bogus, are invalid because they falsify information to bring the price down, or are cancelled soon after purchase.

Graeme Reynolds, director of insurance at the FCA, said that "tight budgets make cheap offers tempting – and scammers take advantage of that".

The FCA is working with social media influencers to warn young drivers about the growing threat of ghost broking.

Don't get ghosted by a policy that doesn't exist. Check the FCA Firm Checker before you buy.

BBC news have reported on the matter. Please read here.

Can you spare 60 seconds?

Counter Fraud Survey 2026/27

It is important for us to understand how effective our Counter Fraud service is. We would therefore be really grateful if you could complete this short survey.

It's only six questions long and should only take a minute to complete. Please scan the QR code to the right.

Thank you for joining us in the fight against fraud in the NHS.

Fraud Awareness & Prevention Training

Our Fraud Awareness and Prevention Training is practical, engaging, and open to all NHS staff – no prior knowledge needed.

Designed around real NHS risks, these sessions give you the confidence to spot fraud, understand the warning signs, and know exactly what to do if something doesn't feel right.

We cover a wide range of key topics, including fraud fundamentals, procurement risks, cyber-enabled scams, payroll and expenses fraud, and tailored sessions for finance, HR, and managers. You can also learn about recruitment fraud, ID checking, and wider fraud risks across the NHS.

Fraud affects us all—and every member of staff has a role to play. Join a session to build your confidence, protect NHS resources, and help safeguard patient care.

Recruitment and ID Checking	3rd December 3pm
Cyber-Enabled Fraud	16th September 10am
Introduction to Fraud Prevention	9th September 10am
Fraud for Finance Staff	9th December 2pm
Fraud Awareness for HR	17th August 2 pm
NEW Imposter Workers and ID checking	15th September 10am
Procurement Fraud	20th October 10am
General Fraud Awareness	9th October 11am
Payroll Fraud	22nd September 1 pm
Fraud Awareness for Managers	11th August 11 am

The sessions are delivered over Microsoft Teams and last around 1 hour. If you would like to book a place on any of the training, please contact: **yhs-tr.audityorkshire@nhs.net**

Bespoke Training Sessions

The Local Counter Fraud Team are always happy to pop along to speak to individual teams. If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

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.