Talking Fraud

Spring 2026

NHS Trust issues warning over AI-generated videos

A major London hospital group has alerted the public to a series of misleading AI-generated videos circulating online that falsely link its doctors to weight-loss products.

The clips, which have appeared on platforms including TikTok and Facebook, depict two individuals dressed in medical scrubs placing adhesive patches on their stomachs and appearing to slim down. The footage is presented as though it features genuine NHS clinicians.

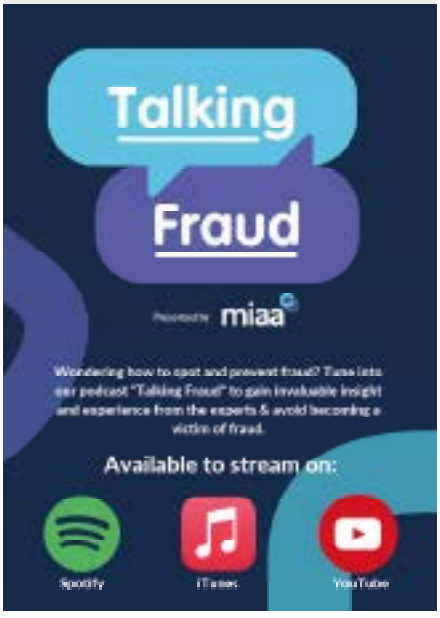
Guy's and St Thomas' NHS Foundation Trust said the people shown in the videos are not connected to the organisation and that the posts wrongly imply its staff endorse the advertised patches.

The Trust stressed that the videos are fabricated and that any accompanying captions suggesting NHS approval are also false.The organisation reiterated that its medical professionals do not promote or support commercial health products of this kind. AI-generated visuals are appearing online in huge numbers. As these tools become more accessible, anyone can create realistic images in seconds, making it harder for people to know what's authentic. Protect yourself;

Use platform tools and security features - Most major social media platforms now include features that flag suspicious content or allow users to report deepfakes. Enabling safety settings, turning on alerts for impersonation attempts, and using official verified accounts for information can help you avoid misleading posts.

Trust credible sources, not random posts - If an image claims to be from a well-known organisation, always check their official website or social media channels. Trustworthy institutions will publish their own statements and will not rely on viral posts to communicate important information.

In this edition:



News

Senior manager jailed after £123,000 fraud

An NHS Counter Fraud Authority (NHSCFA) investigation has led to the jailing of a former NHS senior manager after he and two others defrauded the NHS of more than £100,000.

Alec Gandy, 42, was sentenced to two years and six months' imprisonment at Wolverhampton Crown Court on 16 January 2026. Matthew Lane, 43, was sentenced to 12 months' imprisonment, suspended for 18 months, and 200 hours of unpaid work. Kaylee Wright, 37, was sentenced to 25 days of of rehabilitation activity on the same day.

Alec Gandy,
Picture: West Mercia Police

Gandy was employed by Dudley Integrated Health and Care (DIHC) NHS Trust as a senior manager responsible for the management of Additional Roles Reimbursement Scheme (ARRS) staff in the Primary Care Networks.

He used his position to set up Lane and Wright, who were not DIHC employees, as 'ghost' contractors, with one claiming to be a physician associate and the other an advanced paramedic. Gandy paid a total of £123,000 into their accounts between August 2022 and May 2023.

Their crimes were exposed when a DIHC audit check showed that neither Lane nor Wright were registered to the organisations named on their invoices.

DIHC passed their findings to the NHS Counter Fraud Authority, whose own enquiries showed that both Lane and Wright were receiving payments for these invoices into their respective bank accounts before transferring a large portion of the money back into Gandy's personal account. This was repeated periodically throughout the duration of the fraud.

NHSCFA investigators will now use their powers under the Proceeds of Crime Act (POCA) 2002 to trace and recover these lost funds.

Custodial sentence for credit controller in £300k fraud case

An NHSCFA investigation has led to the jailing of a former NHS credit controller after he and four co-defendants defrauded the NHS out of more than £300,000.

Edias Mazambani, 42, was sentenced to three years and eight months' imprisonment at Southwark Crown Court on Friday 30 January 2026. On the same day George Magaya, 49 was sentenced to three years and two months' imprisonment, Michelle Tengende, 40 was sentenced to 12 months' imprisonment, suspended for two years. She was also ordered to pay costs by 31 December 2026. Rosemary Magaya, 37, was sentenced to 18 months' imprisonment, suspended for two years. Sinqobile Pasipanodya, 43 was sentenced to 18 months' imprisonment, suspended for two years.

The fraud was uncovered by staff within the finance department at Guy's and St Thomas' NHS Foundation Trust after they identified suspicious refund requests relating to monies held on behalf of patients and clients.

Internal investigations revealed the involvement of a Trust employee, Mazambani, who had access to secure financial databases. Further checks confirmed links between him and the bank accounts receiving fraudulent payments.

NHSCFA financial investigators used their powers under the Proceeds of Crime Act 2002 (POCA) to trace the stolen funds. The investigation revealed that Mazambani had facilitated fraudulent refund claims and that money had been transferred to accounts linked to the other defendants.

Ben Harrison, Head of Operations at the NHS Counter Fraud Authority, said: "*Thanks to the vigilance of the Trust's finance team and our investigators' use of Proceeds of Crime Act powers, significant losses were identified and further fraud was prevented.*"

Fraud Prevention: Spotlight on Imposter Fraud

MIAA shares expertise at national conference

Claire Smallman

Claire Smallman, MIAA's Head of Investigations, recently spoke at the NHS Counter Fraud Authority Conference in Leeds, where she shared critical insights into the growing threat of Imposter Fraud.

Claire highlighted a very recent case in which her team was directly involved: the on site arrest of an individual impersonating a healthcare worker at an NHS Trust. This incident underscores the seriousness and potential risk associated with this type of fraud.

Claire explained: *"This is not the first time that we have been made aware of this type of fraud, both regionally and nationally. There may be a real risk about who the imposter actually is and whether they may be a source of potential harm to patients, staff or visitors, let alone a fraud or theft risk. All NHS staff are reminded of the importance of vigilance and the shared responsibility we all have in recognising and reporting suspicious behaviour. If something doesn't feel right — speak up. Your actions could prevent harm and stop fraud in its tracks.*

Some steps to take to help prevent workplace imposter fraud:

- If something doesn't seem right, **don't be afraid to speak up.** Talk to your manager about your concerns as soon as possible, if you can.
- **Don't challenge anyone whom you have concerns about directly.** You don't know how they may react.
- It is everyone's responsibility to be alert to the risk of 'workplace imposters' and to do what they can to protect patients, colleagues, visitors and NHS resources.
- Managers are reminded that they should always **check ID for new staff** on their wards / departments – particularly (but not only) if they have come via an agency.

Minimal checks should include:

- If possible, **check with colleagues** if the worker has come from another area of the organisation, to confirm it's the same individual that they worked with and if they had any concerns.
- **Check their identity badge** to make sure it looks genuine and doesn't feel like it's been altered (i.e. has a different photo been attached, or has it been written over, or does it look like other badges from that agency).
- **Do they actually look like their photo? Does their age look about right?** Be alert to the fact that a worker's formal name isn't always the name which they may have on their agency ID badge, if an ID badge is even provided (i.e. for personal preference or for ease of pronouncing their name).

Fraud Prevention:

Imposter Fraud continued..

Enhanced checks might also include:

Maintaining a ward register signed-off by the Nurse-in-Charge (NIC) to confirm that the ID badge name is the same as the name of the agency worker who has been booked; some organisations even maintain a photo library of agency worker badges to ensure consistency of checks.

Some Trusts provide agency workers with **CIS/Smart Cards,** but to get these they have to bring photo ID (passport, driver's license) with them to verify it is actually them. This can then be used by the NICs when checking ID on the wards.

Some Trusts have a policy whereby all agency workers must go to the Security Office to get access cards for that shift before they can start work. They must provide photo ID (driver's licence, passport) to obtain the access card and must carry the card/ID badge with them while on duty.

Depending on the role the worker will be undertaking, and whether they might present any risks to patients or colleagues**, don't be afraid to not deploy the worker if you genuinely have concerns** that the person is not who they claim to be.

Fraudster 'social engineering' works on the principle that people will be offended if they are challenged, so valid questions from responsible managers are not always asked due to that potential for embarrassment.

Ensuring that only appropriate individuals and workers have access to patients, staff and visitors is far more important than any perceived social discomfort.

Reporting Concerns / Obtaining Advice

If you have any concerns please contact your Anti-Fraud Specialist.

GMP Launches New Anti-Fraud Campaign

Greater Manchester Police are running an anti-fraud campaign. If you would like any of the banners featured in this issue of Talking Fraud, please contact your Anti-Fraud Specialist.

Report Fraud has replaced Action Fraud

Report Fraud has replaced Action Fraud in England, Wales and Northern Ireland.

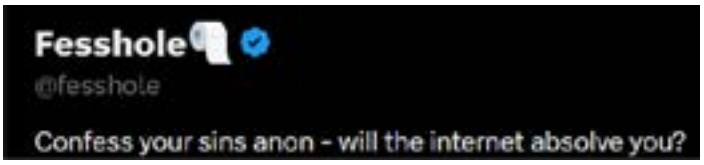
Anyone searching for how to report cybercrime or fraud, or trying to use Action Fraud, will be directed to the new service, which can be accessed online at reportfraud.police.uk or by calling **0300 123 2040.**

Report Fraud provides:

- A clear and simple reporting process to tell the police about cybercrime and fraud
- Guidance on what to report and how information is used
- Further support information for victims

The launch of Report Fraud marks the beginning of a new service to improve the national response and, most significantly, the development of a more comprehensive intelligence picture of cybercrime and fraud affecting people and businesses, resulting in a faster response from law enforcement agencies.

Spotlight: Is it fraud?



Cultural phenomenon Fesshole allows the public to confess their sins and misdeeds on social media and be judged on their actions by the internet. Many of these are not suitable for this professional publication, but we can judge some of their confessions as to whether they constitute fraudulent activity or not.

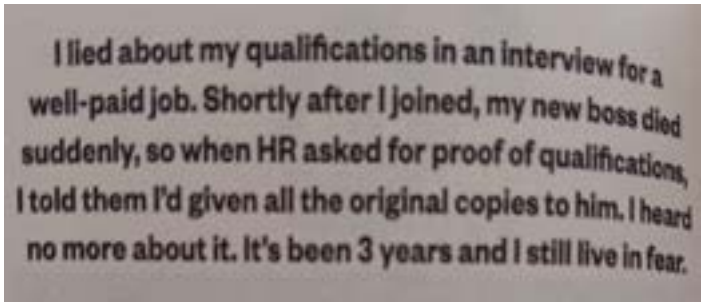
Is this fraud?

This is fraudulent behaviour, and staff within the NHS have been prosecuted, and continue to be prosecuted, for such activity.

In one case, an NHS employee lied about the deaths of three family members: a sister, a brother and a cousin in order to take paid time off from his NHS Trust.

None of them had died, so he was misrepresenting the situation, to abuse the Trust sickness absence process, which is Section 2 of The Fraud Act 2006 (Fraud by False Representation).
He avoided prison but received a 12-week prison sentence suspended for 18 months, as well as conducting 240 hours of unpaid community work, and had to pay the Trust £5K.

Is this fraud?



Lying about your qualifications as part of a job recruitment process is fraudulent behaviour.

Several NHS staff have purported to be more qualified than they are, and have been prosecuted for fraud, as they are literally misrepresenting themselves (often with qualifications not even relevant to the job they are applying for). Section 2 of the Fraud Act 2006 is “Fraud by False Representation”.

- A Chief Executive had lied about having a degree, and was sentenced to a 12 month prison sentence, suspended for two years, after faking his qualifications to obtain the £100K+ a year post
- Another prospective NHS Chief Executive was not awarded the role when it turned out that his Law Degree had not been completed. He was dismissed from his existing role of Trust Director of Planning and Performance.
- The Chair of an NHS Trust also lied about a number of his academic qualifications and was sentenced to two years in prison.

If you lie about your qualifications, or experience, on a CV, application form, or even in the interview itself, you are committing an act of fraud.

In the NHS you are likely to be investigated, and face sanctions, if you commit this behaviour. As well as a criminal sanction, this could also a disciplinary investigation, referral to your regulatory body, and even financial compensation / repayment.

If you suspect that anyone is committing fraud or another economic crime against the NHS, speak to your local Anti-Fraud Specialist or contact NHSCFA using their website to report online: www.cfa.nhs.uk or telephone the 24-hour reporting line **0800 028 40 60.**

Fraud alerts

CAPTCHA scam alert

Genuine CAPTCHA

A CAPTCHA is a small test on a website used to tell whether the user is a real human or an automated bot.

Cybercriminals are increasingly exploiting CAPTCHA. Recent reports show that fake CAPTCHA scams have surged, with attackers mimicking legitimate “I’m not a robot” checks from services like Google reCAPTCHA or Cloudflare. In many cases, simply clicking the fake prompt can trigger the silent installation of malware, such as info stealers that harvest passwords, browser data, and financial details.

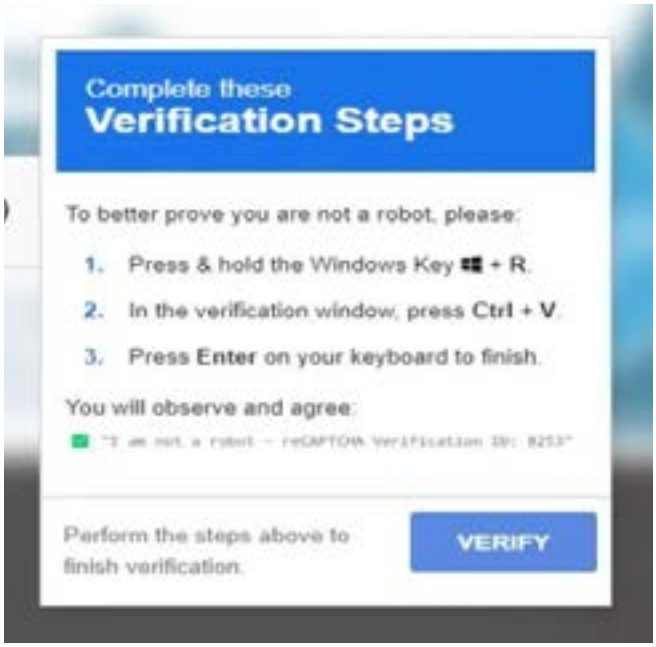
Some scams go even further, instructing victims to perform actions no genuine CAPTCHA would ever require—such as opening the Windows “Run” dialog and pasting in a text command. Following these steps executes hidden PowerShell scripts that install remote access tools and other malicious payloads, giving attackers direct access to a victim’s device.

How to Spot a Fake CAPTCHA

While fake CAPTCHAs are designed to look convincing, there are clear warning signs:

- Unusual instructions - A legitimate CAPTCHA will never ask you to press keyboard shortcuts, open system tools, or paste commands. If you see instructions to use Windows “Run” or copy/paste text, it’s a scam.
- Strange or suspicious website domains - Real CAPTCHA components load from trusted providers such as google.com/recaptcha. If the page URL looks unrelated or suspicious, treat it as a red flag.
- Placement in unexpected locations - CAPTCHAs usually appear during login, sign up, or checkout processes—not as random pop ups while browsing. Unexpected prompts should be treated with caution.
- Redirect chains or multiple CAPTCHA screens - Fake verification pages often redirect users through several screens, each adding more steps designed to manipulate you into running malicious commands. Legitimate CAPTCHAs do not do this.

Scam CAPTCHA



Staying Safe

If something feels off, stop immediately—genuine CAPTCHAs never require system level actions, and never request personal information such as passwords or payment details. Stick to reputable sites, avoid interacting with CAPTCHAs on pages offering pirated or “free” content, and always check the URL before clicking.

Fake CAPTCHA scams work because they exploit routine behaviour. Staying alert to the red flags can prevent malware infections, data theft, and financial loss.

Useful Sources of Information

• MIAA Fraud alerts, blogs, and newsletters - Our fraud alerts and newsletters bring together rich sources of information relating to the latest scams and fraud cases so that our readers can be vigilant in work and at home.

• NHS Counter Fraud Authority - The NHS Counter Fraud Authority (NHSCFA) is a special health authority tasked to lead the fight against fraud, bribery and corruption in the NHS.

• CFA Report Fraud - You can use this online form to report fraud against the Department of Health and Social Care (DHSC) and the wider health group, including the NHS in England and Wales.

• Take Five to Stop Fraud – Take Five is a national campaign offering straightforward, impartial advice that helps prevent email, phone-based and online fraud - particularly where criminals impersonate trusted organisations.

• The National Cyber Security Centre – Organisation helping to make the UK the safest place to live and work online.

• Report Fraud - Report Fraud has replaced Action Fraud as the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland.

• NHS Digital – Guidance on Phishing Emails - Find out how you can stay safe and vigilant against phishing emails, including advice on how to spot a suspicious email and how to report it.

Contact your Anti-Fraud Specialist

Darrell Davies
Regional Assurance Director (Anti-Fraud)
07785 286381
Darrell.Davies@miaa.nhs.uk

Paul Bell
Head of Anti-Crime Services
07552 253068
Paul.Bell@miaa.nhs.uk

Claire Smallman
Head of Investigations
07769 304145
Claire.Smallman@miaa.nhs.uk

Sarah Bailey
Anti-Fraud Specialist
07721 488602
Sarah.Bailey@miaa.nhs.uk

Linda Daisley
Anti-Fraud Specialist
07570 147318
Linda.Daisley@miaa.nhs.uk

Kevin Howells
Anti-Fraud Manager
078257 32629
Kevin.Howells@miaa.nhs.uk

Carl Jervis
Anti-Fraud Specialist
07785 601900
Carl.Jervis@miaa.nhs.uk

Paul Kay
Anti-Fraud Specialist
07990 082328
Paul.Kay@miaa.nhs.uk

Phillip Leong
Anti-Fraud Specialist
07721 237352
Phillip.Leong@miaa.nhs.uk

Virginia Martin
Anti-Fraud Specialist
07551 131109
Virginia.Martin@miaa.nhs.uk

Karen McArdle
Anti-Fraud Specialist
07774 332881
Karen.McArdle@miaa.nhs.uk

Paul McGrath
Anti-Fraud Manager
07584 774761
Paul.McGrath@miaa.nhs.uk

Claire Taylor
Anti-Fraud Specialist
07552 297469
Claire.Taylor@miaa.nhs.uk

Andrew Wade
Anti-Fraud Specialist
07824 104209
Andrew.Wade@miaa.nhs.uk