Talking Fraud

Spring 2025

Are we becoming more dishonest?

Recently, there was an interesting article on the BBC News website on 23 January 2025: https://www.bbc.co.uk/news/articles/cdxnkydje7no about whether, as a nation, we are becoming more dishonest (or, perhaps, less intolerant to certain dishonest acts).

The article is worth a read; it references a 2023 academic study which concluded that, "*overall, there has been a decline in honesty*" across the UK.

This study also suggested that, when it came to more serious dishonesty of a criminal nature, there had been a noticeable fall in the number of people who said particular acts were never acceptable, when compared to a similar study in 2011. These included buying stolen goods, accepting a bribe and falsifying a benefits claim.

The latter saw the biggest decline, dropping 18 percentage points from 85% to 67%.The article also looked at what might be behind a possible decline in general honesty levels, if true, and points towards a variety of factors including social media toxicity (whatever that means…), corrupt / dishonest organisations in the public eye (the Post Office Horizon scandal and its treatment of sub-postmasters could be cited as an example), as well as an almost never-ending catalogue of politicians, of various political colour, demonstrating questionable personal integrity and honesty.

Significant adverse economic factors over the past several years, with high inflation and the cost-of-living crisis, could easily be added into this mix. All of these elements feed into the long-established notion of the 'Fraud Triangle' (The Fraud Triangle: Why People Commit Fraud).

So, are we at MIAA seeing more dishonesty? An interesting question which requires a two-part answer. We're certainly seeing more dishonesty – but that's generally from professional criminals who are, by definition, dishonest to start with and who are finding more ways to commit offences.

In this edition:

News

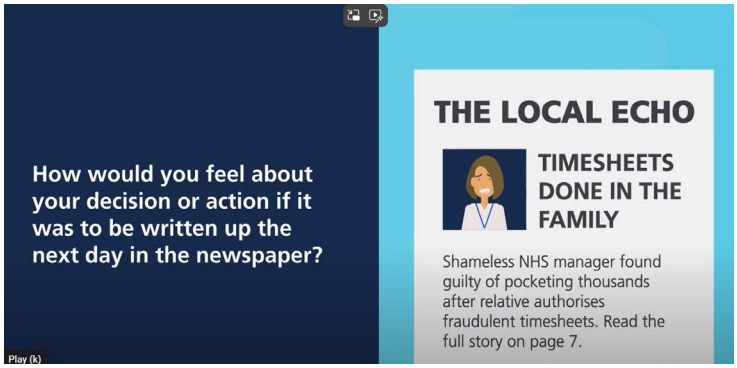
Are we becoming more dishonest? cont.

However, we're not necessarily seeing an increase in dishonesty levels from 'opportunistic' fraudsters.

By that, we mean those individuals who are not professional fraudsters by nature and who perhaps spot an opportunity to submit an inflated expense claim or lie on a CV / job application, at a time when they are experiencing particular financial pressures.

Either way it's looked at, we're unfortunately not currently seeing any less fraud regardless of whatever motivations lie behind it.

Conflicts of Interest



Please take the time to watch our short video about declaring potential conflicts of interest. In a worst case scenario, an undeclared conflict of interest might result in a fraud investigation. You should familiarise yourself with your organisation's policy and ensure you fully comply with all requirements. Watch now: https://ow.ly/o69850V2TOk

NHSCFA's Annual Strategic Intelligence Assessment

Alex Rothwell, NHSCFA CEO

The NHS Counter Fraud Authority published their annual Strategic Intelligence Assessment in October 2024, and while some of what it says is obvious to the counter fraud community working 'on the ground', it does make interesting reading.

In the assessment they report on their *"annual strategic intelligence assessment to estimate fraud losses, identify possible threats, vulnerabilities, and facilitators, and evaluate the risk of fraud to the NHS."*

The document provides the NHSCFA's annual estimate of the fraud loss to the NHS, which now stands at £1.316 billion (rising from £1.26 billion) - the highest level it has ever been estimated to be, although it has reduced slightly as a percentage of the overall NHS budget.

In tandem with this, the number of reported frauds in 2023/24 also stands at the highest ever level, with 6,367 reported frauds in the year (26% more than in the prior year) to NHSCFA. Nearly half of these reports of fraud relate to NHS staff, though the valuation is only a small element of the £1.316 billion.

As ever, NHS organisations and employees need to remain vigilant to fraud, and the potential losses to the NHS, and work with their Anti-Fraud Specialist to raise awareness of NHS fraud and together promote a strong counter-fraud culture.

News

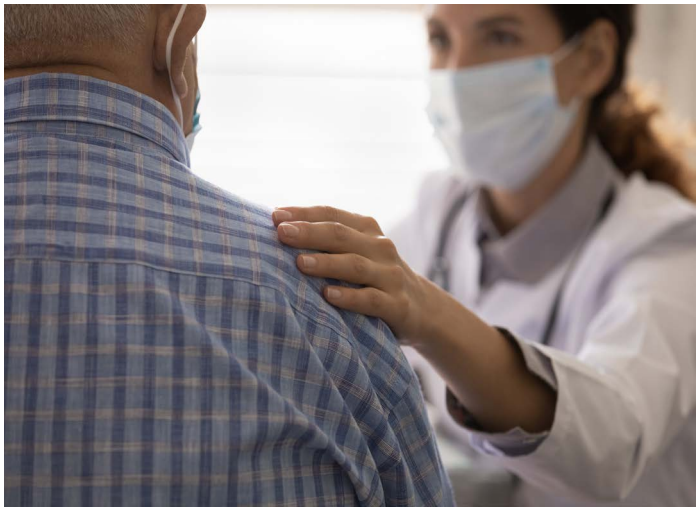
Cancer Nurse Struck Off for Financially Grooming Patient

Anita George, a nurse who initially seemed trustworthy, has been struck off the nursing register for financially exploiting Ian Percival, a cancer patient she cared for. George moved into one of Percival's properties to help look after his wife, Margaret, who had mobility issues. Over time, however, the family grew concerned about the influence George had over Ian, especially after his cancer diagnosis.

Despite initially reassuring the family with her professional credentials, George's behavior became increasingly suspicious. She focused her attention on Ian, refusing to care for Margaret, and over time began manipulating him for financial gain. Ian had given her nearly £15,000 in cash, shares, a car, and a property worth hundreds of thousands of pounds. George even listed herself as Ian's next of kin on his medical records, managing his hospital appointments and medical care without his family's knowledge.

In December 2024, the Nursing and Midwifery Council (NMC) concluded that George had abused her position of trust as a nurse, motivated by financial gain. The NMC struck her off, its most severe sanction. The case also highlights the growing issue of financial exploitation of the elderly, with the charity Hourglass reporting an alarming rise in such cases.

Swansea Bay University Health Board, which oversees the hospital where George worked, has expressed regret and is reviewing the case for potential failures in care. This incident serves as a stark reminder of the risks of financial abuse, especially when elderly individuals are isolated and vulnerable.



Unauthorised software on NHS devices is a security risk

"Following serveral high profile cyber incidents at a number of hospitals in Merseyside, we want to remind everyone of the importance of adhering to your Trust's digital policies, particularly regarding the use of hardware and software on NHS devices", says Darrell Davies, MIAA's Regional Assurance Director (Anti-Fraud)

There have recently been instances of unauthorised software installations, including the use of mouse movers (also known as "mouse jigglers"). These devices are designed to keep a desktop or laptop in active mode by automatically moving the cursor every few seconds, preventing the device from going idle. While this may seem harmless, it creates the false impression that you are actively working, even when you are not.

Why is this a concern?

Violation of Trust Policies: The installation and use of unauthorised software, including mouse movers, can directly contravene a health body's established digital security policy.

Increased Cybersecurity Risks: These types of software can create vulnerabilities that may be exploited by cybercriminals, increasing the risk of cyberattacks and data breaches.

Potential for Misconduct: If you are found using unauthorised software to falsely show activity when you are not working your contracted hours, this could be considered an attempt to deceive your employer. Such actions may lead to a disciplinary investigation, and in some cases, a criminal investigation could also be initiated.

What you need to do

If you have installed any unauthorised software, including a mouse mover, please remove it immediately.
If you need assistance ensuring compliance with organisation policies. policies, or if you have concerns about your device, please reach out to your IT department for support.

News

NHSCFA CEO Alex Rothwell Speaks at House of Commons

Alex Rothwell, Chief Executive of the NHS Counter Fraud Authority (NHSCFA), recently provided testimony at a hearing for the House of Commons Public Bill Committee, which is reviewing the proposed Public Authorities (Fraud, Error and Recovery) Bill. The Bill, if passed, aims to enhance efforts to combat fraud within the public sector and establish new measures to recover financial losses in cases where no criminal investigation is pursued.

Rothwell expressed his support for the bill, emphasising its potential to strengthen the tools available for tackling public sector fraud. He remarked, *"It was a pleasure to appear as a witness for the Public Bill Committee. If passed, this bill will strengthen measures to tackle public sector fraud, including powers to recover losses where no criminal investigation ensues."*

Mr Rothwell also highlighted the importance of ensuring that any action taken is proportionate and backed by appropriate safeguards. However, he stressed the crucial point that, "*when public money has been lost, we want to recover it. Every penny saved contributes to better healthcare outcomes."* He also spoke about the challenges the authority has faced in addressing public sector fraud but praised the role of the NHSCFA in supporting the professionalisation of counter-fraud efforts across the public sector.

We will provide more information to our clients as the bill progresses through Parliament.

For those interested in watching the full hearing, it is available online here: Watch the hearing.

A collaborative approach to recovery

Sarah Bailey

At MIAA, we thought it might be informative to share a recent success story that highlights the importance of diligent fraud investigation and the power of collaboration across NHS departments and functions. We had been working on an investigation at a Trust into an ex-employee who was found to have been working elsewhere while off sick.

During the course of this investigation, a significant payroll error was identified, whereby the individual had been mistakenly paid over £9,000 due to an oversight by Payroll. The Trust had invoiced the individual, with a view to recovering the overpayment by mutual agreement. This had been unsuccessful. As part of the investigation, our Anti-Fraud Specialist, Sarah Bailey, was scheduled to conduct an Interview Under Caution (IUC) with the subject. After the IUC, Sarah challenged the individual, who initially claimed they had not received the invoice for the overpayment.

Sarah took the opportunity to explain that they had been paid money to which they were not entitled and that repayment was required; otherwise, further procedural action might be taken. Wrongly retaining monies to which someone is not entitled, even if they came into possession of that money as a result of a genuine error, can be viewed as a criminal offence. However, Sarah's intervention, fortunately, moved matters along promptly. Thanks to this action, the Trust subsequently confirmed that the full amount had been paid back. The Head of Financial Services expressed gratitude for Sarah's involvement, noting that her efforts had been crucial in recovering the funds. In addition to this, an overpayment exceeding £13,000 had been raised in connection with the subject's actions, while off sick from their NHS role.

Woman scammed out of £700,000 by fraudster posing as Brad Pitt

How to spot AI images being used for fraud

A recent Ofcom study revealed that more than half of 12-15-year-olds have used AI tools, with 45% using them just for fun. However, while AI can be entertaining and creative, it's also being exploited by fraudsters to deceive people.

One recent example is a French woman who was scammed out of £700,000 by a fraudster posing as Brad Pitt. The scammer used AI-generated images of the actor, claiming that Pitt needed money for cancer treatment after his bank account was frozen. This incident is part of a worrying trend, as similar scams have involved AI images of celebrities like Brad Pitt before. It must be noted, however, that many of these images are not particularly convincing - and can even be quite comical - which should be the first 'red flag' to everyone!

Though many young people believe they can easily spot fake images online, the technology behind these AI images is improving, making it harder to differentiate between real and fake.

To help spot AI-generated images, here are some tips:

- **Look at the details** – The quality of AI images is getting better all the time, but they can have a few giveaways. AI images are produced using data taken from other pictures, so AI programs can struggle with details. Look at details such as the fingers to see if they look natural and logos and images can also be a giveaway as AI can often get these wrong.

- **Check for perfection** – AI images often lack details that can be found in real pictures and can have an overly polished, "airbrushed" look. AI images are quite often set in a perfect location or fantasy.

- **Check the source** – Images from reliable, trusted outlets are more likely to be authentic.

This will identify other places on the internet that the photo exists, and can be very helpful when trying to determine if a picture is AI or real. Generally, AI photos will appear in fewer places than real ones, so will show up less frequently when you run a reverse image search.

As scams become more sophisticated, it's more important than ever to stay vigilant online.

How to check the source of images

Bing Visual Search

1.Visit Bing.
2. Click on the "Images" tab and look for the camera icon in the search bar.
3. Upload your image or paste the URL to search for similar images.

Google Images

Click on the camera icon in the search bar (on the right side). You can either:
1. Paste the image URL (if the image is online) or
2. Upload an image from your device by clicking "Upload an image" and selecting the file from your computer.

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.

• Action Fraud - Action Fraud is 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

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

Neil McQueen
Anti-Fraud Specialist
07721 237353
Neil.McQueen@miaa.nhs.uk

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