tiaa

FRAUD STOP

Issue 8

The Failure to Prevent Fraud Offence – Is Your Organisation Ready?

→ SEE PAGE 2

NHS Fraudsters

Cases in Court

→ SEE PAGE 4

A rise in Quishing scams

→ SEE PAGE 6

Introduction

Fraud is deception carried out for personal gain, usually for money, but can also involve the abuse of a position of trust.

While those who commit fraud against the NHS and the wider healthcare sector are a small minority, their actions have a serious impact on us all.

The NHS Counter Fraud Authority estimates that the healthcare sector is vulnerable to £1.346 billion worth of fraud each year. This is taxpayers' money taken away from patient care and into the hands of criminals.

This edition of Fraud Stop includes guidance on the new 'failure to prevent fraud' offence, a spotlight on the increase in dual working fraud cases, a round-up of court cases, and do you know about quishing?

Failure to Prevent Fraud Offence

The new 'failure to prevent fraud' offence, which was introduced as part of the Economic Crime and Corporate Transparency Act (ECCTA) 2023 came into effect on the 1 September 2025.

Under the offence, an organisation may be criminally liable where an employee, agent, subsidiary, or other "associated person," commits a fraud intending to benefit the organisation and the organisation did not have reasonable fraud prevention procedures in place. In certain circumstances, the offence will also apply where the fraud offence is committed with the intention of benefitting a client of the organisation. It does not need to be demonstrated that directors or senior managers ordered or knew about the fraud.

NHS Foundation Trusts, NHS Trusts, Integrated Care Boards and large organisations in the independent healthcare sector are in scope for the offence.

The offence sits alongside existing law; for example, the person who committed the fraud may be prosecuted individually for that fraud, while the organisation may be prosecuted for failing to prevent it.

The offence will make it easier to hold organisations to account for fraud committed by employees, or other associated persons, which may benefit the organisation, or, in certain circumstances, their clients. The offence will also encourage more organisations to implement or improve prevention procedures, driving a major shift in corporate culture to help prevent fraud.

ECCTA introduced amendments to the identification doctrine for economic crimes. The identification doctrine is the means by which an organisation can be found criminally liable for the actions of an individual. Under ECCTA, a company or partnership commits an economic crime offence where the offence is committed with the involvement of a "senior manager." This expands the group of individuals who can trigger liability for the organisation. This makes charging decisions for prosecutors, and subsequent prosecution of companies, and partnerships more straightforward.

The NHS Counter Fraud Authority (NHS CFA) recommend that organisations review their fraud prevention procedures, be able to demonstrate that reasonable procedures for the prevention of fraud are in place and ensure that fraud prevention procedures are informed by the NHS CFA requirements and the six principles that underpin the fraud prevention framework.

- **Top level commitment**
- **Risk assessment**
- **Proportionate prevention procedures**
- **Due diligence**
- **Communication (including training)**
- **Monitoring and review**

More information can be found at: https://cfa.nhs.uk/fraud-prevention/failure-to-prevent

Dual Working Fraud

A more flexible approach to work following the pandemic has offered benefits to both employers and employees, but new working arrangements present a greater risk of dual working fraud, also known as polygamous working. Cases are being identified of individuals working multiple full time jobs simultaneously. This could involve an individual failing to disclose another job or being paid for hours not worked.

The NHS Counter Fraud Authority (CFA) has identified a growing trend of fraud offences in relation to staff working elsewhere during their contracted business hours. Individuals are falsifying employment history and references to support their application and are actively seeking home-based employment.

The Public Sector Fraud Authority has issued guidance in respect of dual working fraud with advice on risk indicators which include:

Irregular documentation of work schedules – unrealistic or incomplete timesheets

Unauthorised and inconsistent working patterns – unexplained absences, missing meetings, lack of contact or response

Poor performance – missed targets and low quality output

Prevention advice

- Prior to employment, personal and professional references should be checked
- Agencies who provide staff should provide assurance that their pre-employment screening practices are robust
- Ensure conflicts of interest have been declared which includes business interests and other employment, paid or unpaid, in line with the organisation's policy
- Employment contracts should be clear on when contracted hours should be worked, the location of the work and make reference to the organisation's policy on multiple assignments
- Agree and document flexible working arrangements
- Ensure timesheets and absence logs are updated accurately and if possible, independently verified
- Be proactive in performance management - set clear deadlines and objectives

Cases in Court

Former GP Practice Manager sentenced for £144K fraud

An NHS Counter Fraud Authority (CFA) investigation has resulted in a former NHS GP Practice Manager receiving a suspended jail sentence after she pleaded guilty to defrauding the health service of more than £144,000.

The fraudster received her sentence at a Crown Court hearing on Monday 15 September 2025. She had previously pleaded guilty to two counts of fraud by abuse of position at the Magistrates Court on 15 August 2025.

She was sentenced to two years' imprisonment, suspended for 18 months, as well as 20 hours of rehabilitation. She will also be electronically tagged for four months.

NHS CFA investigators will now use their powers through the Proceeds of Crime Act 2002 (POCA) to reclaim some of the stolen funds.

In her Practice Manager role, she had control of all banking, including salary payments and paying locum doctors when they submitted invoices.

In January 2021, she began fraudulently obtaining funds from the practice by transferring money from the surgery to her own bank account. She hid these payments by labelling them as payments to others.

She paid herself salary increases and overtime payments beyond the agreed terms. These began as minor amounts but grew into significantly larger sums, none of which were authorised by the practice partners.

In total, she stole £144,864.13 from the practice and attempted to cover the payments by creating false invoices, in the hope that they would go undetected.

Trainee Psychologist in court for expense claim fraud

Following an investigation by TIAA Anti-Crime Specialists, on 13 October 2025, an NHS Trainee Psychologist was convicted of fraud by false representation and sentenced to 26 weeks imprisonment, suspended for 12 months, ordered to undertake 250 hours of unpaid work and pay the NHS £12,605.94 in compensation.

The fraudster was employed via an agency working at an NHS Foundation Trust. Between 11 May 2021 and September 2022, she submitted false mileage expense claims claiming to have attended her place of work at when no such journey was undertaken. Furthermore, she forged the authorising signature on claim forms.

She pleaded 'guilty' and was sentenced at the Magistrates Court, where the Judge said "the aggravating factors are that you held a position of trust and abused that position to make false expense claims. The worst part is that the victim was the NHS."

The Judge ordered her to pay compensation of £5,418 for the false expenses claims and £7,187 for the cost of the investigation to the NHS.

Suspended jail sentences for Personal Health Budget holder and carer

In June 2025 a Personal Health Budget holder and his carer were convicted at Crown Court for defrauding the NHS by abusing a Personal Health Budget (PHB).

Following allegations raised, an investigation was carried out which found the holder of the PHB, and his carer had conspired together to defraud the NHS out of over £17,000 by submitting false invoices and incorrect records in relation to the PHB holder's care needs. They were both charged having admitted fraud by false representation and making or supplying an article for use in fraud. The fraud ran for 12 months between January 2022 and January 2023.

The carer was sentenced to 15 months imprisonment, suspended for 18 months and was ordered to complete 20 rehabilitation activity hours and 150 community work hours. He was ordered to repay fraud losses of £7,200.00 to the NHS over 3 years. The PHB holder was further sentenced to 15 months imprisonment, suspended for 18 months and ordered to complete 20 rehabilitation activity hours. He was also ordered to repay fraud losses of £1,800.00 over 3 years.

Four men jailed for £6m bribery and corruption against NHS Scotland

Four men were sent to prison on 5 June 2025 for a combined 29 years for fraud, bribery, and corruption against NHS Scotland.

Two former NHS employees were sentenced to eight years and six years respectively and two directors of a firm were jailed for eight years and seven years respectively.

The NHS Counter Fraud Authority reported that this was a landmark case for NHS Scotland Counter Fraud Services who led the investigation with support from Police Scotland and the NHS Counter Fraud Authority's Digital Forensic Unit.

Investigators collected over 4,000 items of evidence, including dozens of mobile phones and laptops. More than 250 witnesses were also interviewed during the investigation.

The case began with an enquiry over the theft of mobile telephones and bills for their use abroad.
Further investigations identified that between 2010 and 2017, the two former NHS employees accepted bribes, hospitality and cash incentives worth £100,000 in exchange for sensitive information that led to the awarding of contracts worth £6 million.

The contracts related to the supply, installation and maintenance of telecommunications and video conferencing throughout NHS Scotland.

The investigation identified that many of the incentives were later paid for by the NHS through false, inflated or duplicated invoices.

Police Scotland and the NHS Counter Fraud Authority's Digital Forensic Unit (DFU) supported Counter Fraud Services in executing search warrants at NHS and the firm's premises, where digital and physical evidence was retrieved for examination.

The DFU created an on-site forensic image of the firm's servers, and the remaining digital devices were taken to the DFU office for analysis.

Tens of thousands of text messages and emails were reviewed. They uncovered deliberate acts to divert or manipulate NHS funds for personal gain at the expense of patient care and public trust.

Former NHS mental health nurse jailed for defrauding the NHS

A former nurse employed by a mental health NHS Foundation Trust was convicted at Crown Court on 15 May 2025 of fraud by abuse of position after falsely claiming he had worked 185 shifts for which he received £72,632.72 in wages and holiday pay. He had entered a guilty plea at an earlier hearing and was jailed for 18 months.

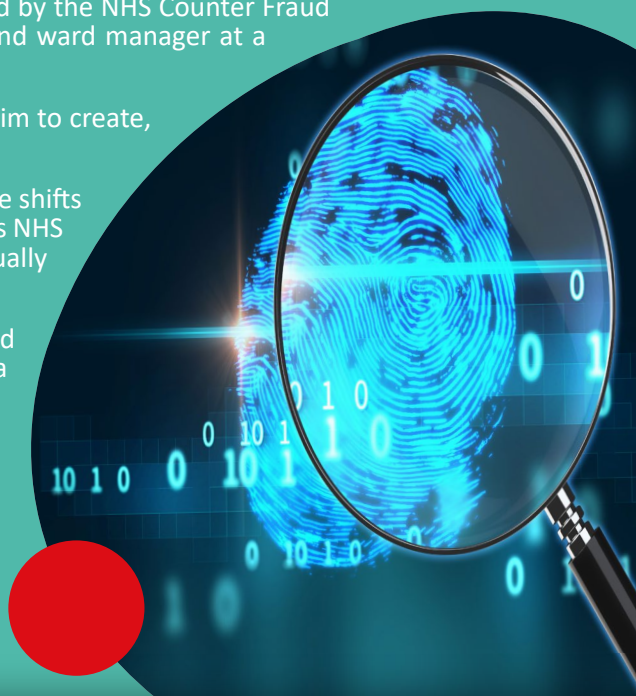
An investigation, led by the Trust's Counter Fraud Specialist and supported by the NHS Counter Fraud Authority, found that the fraudster had abused his position as a nurse and ward manager at a mental health unit.

As a manager, he had access to the shift booking system, which allowed him to create, assign and authorise additional shifts.

Starting in April 2020, the former nurse began creating backdated overtime shifts in his own name. These were entered into the NHS Staff Bank, which allows NHS employees to pick up additional shifts on top of their contracted hours, usually to cover for NHS staff shortages.

He mainly claimed for night shifts which are paid at a higher rate and because they were created after the event, they did not appear on any rota thus raising no suspicion. This continued until October 2021.

In November 2021, irregularities were identified in respect of additional shifts claimed for payment, which led to him being suspended from duty and a criminal investigation was opened.



Quishing alert - £3.5 million lost to fake QR codes

Action Fraud, the National Fraud & Cyber Crime Reporting Centre, is urging people to look out for rogue QR codes as £3.5 million was lost to fraud between April 2024 and April 2025.

Quishing is a form of phishing (also known as QR Phishing) where a fraudulent QR code is scanned, designed to steal personal and financial information. Action Fraud advice is to stay vigilant and double check QR codes to see if they are malicious, or have been tampered with, before scanning them online or in public spaces.

Quishing happens most frequently in car parks, with criminals using stickers to tamper with QR codes on parking machines, but quishing also occurred on online shopping platforms, where sellers received a QR code via email to either verify accounts or to receive payment for sold items.

Action Fraud has provided the following advice:

- QR codes used in pubs or restaurants are usually safe to scan.
- Scanning QR codes in open spaces (like stations and car parks) might pose a greater risk. Check for signs that codes may have been tampered with (usually by a sticker placed over the legitimate QR code). If in doubt, do not scan them: use a search engine to find the official website or app for the organisation you need to make a payment to.
- If you receive an email with a QR code in it, and you are asked to scan it, you should be cautious due to an increase in these types of quishing attacks.
- It is recommended that you use the QR-scanner that comes with your phone, rather than using an app downloaded from an app store.

Further information at: New quishing alert: https://www.actionfraud.police.uk/news/qr-codes

If you have been a victim of quishing, use the link above to report to Action Fraud and contact your bank immediately if you think you may have lost money.

To report fraud, contact your Anti-Crime Specialist or

→ Andrew Ede, Head of Investigations – Healthcare, Tel 07814 285177 or

email: andrew.ede1@nhs.net / andrew.ede@tiaa.co.uk, or fraud@tiaa.co.uk

You can also report via the NHS Counter Fraud Authority. You can call the anonymous, 24-hour reporting line on 0800 028 4060 or use the confidential online reporting form. www.cfa.nhs.uk/reportfraud