THE MANY FACES OF NHS FRAUD

FRAUD *INSIGHT*

JANUARY 2022

auditone
assurance . counter fraud . advisory

NATIONAL CASE: IT WASN'T ME IT WAS MY RECRUITMENT AGENCY

A 29 year old woman who cheated her way into an NHS job with lies on her CV and bogus references tried to shift the blame onto one of the recruitment agencies she was registered with. She pretended she had a master's degree in molecular biology and experience leading a charity to land a senior job with an NHS Clinical Commissioning Group. She was put in charge of delivering programmes for urgent care patients in the borough. However, when challenged over her failing performance she made a string of false accusations of bullying, assault, racism and that someone at a recruitment agency had been responsible for the falsifications. Croydon Crown Court heard that the subject had worked for charity Action Aid, collecting money in the street and going door-to-door asking for donations. However, on her CV, she pretended her role had been much more senior when applying for the Commissioning and Programme Lead for Urgent Care post in December 2019. She invented the master's degree qualification as the job advert had suggested one would be preferable and burnished her credentials with false references that she had either written herself or organised for others to write. She was jailed for 12 months and will need to repay the £13,171 she earned in wages back to the NHS.

NEWS: AUDITONE COUNTER FRAUD TEAM IN THE SPOTLIGHT

auditone
assurance . counter fraud . advisory

Publicity has always been a big part of raising awareness of NHS fraud, so it was with great enthusiasm that Paul Bevan, Counter Fraud Specialist and Michelle Watson, Head of Operations (Reactive) accepted an invitation to be interviewed about their work by the Newcastle Chronicle. The interview followed on from the successful awareness campaign that the counter fraud team ran for International Fraud Awareness Week (IFAW) between 14 and 20 November 2021. This campaign, supported by the majority of AuditOne clients, and conducted primarily via Twitter provided fraud awareness information to a potential audience in excess of 450k. Anyone who has not yet seen the article can access it by clicking the following link: Click here to read the Newcastle Chronicle article

SCAM ALERT: WHATSAPP FAMILY MEMBER SCAM

New data from Action Fraud, reveals a new emerging threat where victims are being targeted on WhatsApp by criminals pretending to be someone they know. Criminals will typically claim to be a family member and will usually begin the conversation with "Hello Mum" or "Hello Dad". They will say that they are texting from a new mobile number as their phone was lost or damaged and will go on to ask for money to purchase a new phone, or claim that they need money urgently to pay a bill. The criminal will supply their bank details for payment, with some coming back with further demands for money. Criminals are successful in their approach as they are exploiting the emotional vulnerability of the public in an attempt to deceive victims.

How to protect yourself

- If you receive a similar message that's asking you for money, speak with the person over the phone to verify they are who they say they are.
- You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions. Action Fraud advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.
- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

NATIONAL CASE: FORMER NURSE JAILED FOR FRAUD

A former nurse from Hartlepool, was sentenced to 14 months in prison for four counts of fraud.

She admitted taking the bank card of an 84-year-old patient while working on his ward at an NHS hospital. She callously used the card to spend over £1,700 on herself including a bed costing £699, wallpaper and items from Amazon and she paid off a £900 personal loan. The victim died just days after her crimes were uncovered by his relatives.

The court heard that her actions had caused significant hurt to the victim's family at a very distressing time.

SCAM ALERT: LOTTERIES - YOU COULD BE THE UNLUCKY ONE

New data from Action Fraud, reveals almost £1 million has been lost to lottery fraud in the past seven months. Criminals will contact unsuspecting victims informing them they have won a lottery or prize draw. The victim is then informed that they will need to pay an advance fee in order to receive their winnings. In reality, the winnings are non-existent and it is an attempt to steal the victims money, personal or financial information. Temporary Detective Chief Inspector Craig Mullish, from the City of London Police, said: "*Criminals are experts at impersonating organisations and will mimic a number of well-known prize draws to take advantage of unsuspecting victims. Remember, you can't win a draw that you haven't entered so if you're contacted out of the blue claiming you've won a prize draw but can only access these winnings by paying an advance fee: stop and think as it's likely to be a scam. This could protect you and your money.*"

Clara Govier, Managing Director of People's Postcode Lottery said: "*Fraudsters often impersonate trusted brands like ours. Thankfully, we can all help protect ourselves our families and neighbours by following, and sharing, some straightforward advice. Please remember, People's Postcode Lottery will never ask for any kind of payment to claim a prize,* ***you can't win if you don't play****, and we don't offer discount cards.*

How to protect yourself

Action Fraud advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.

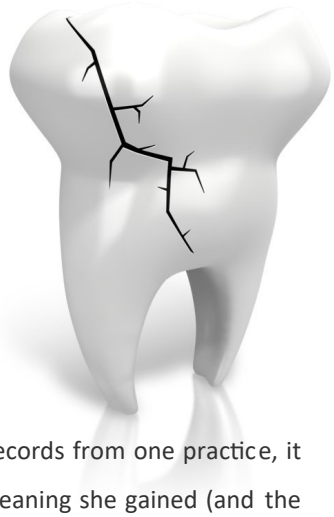
- **Stop:** Unsolicited offers of large sums of money in return for a small upfront payment should always raise a red flag. Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? Remember, you can't win a prize in a competition you didn't enter. It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

You can find further protection advice around lotteries and competition on the Gambling Commission's website.

NATIONAL CASE: NHS MANAGER SENTENCED FOR £30K TRAVEL FRAUD

A former manager for NHS Improvement (now NHS England and NHS Improvement) was sentenced to 14 months' imprisonment, suspended for 18 months for defrauding the NHS of over £30k. He also received a 15-day Rehabilitation Order and was ordered to carry out 200 hours of unpaid work. He pleaded guilty to two charges at Thames Magistrates Court, one of Fraud by False Representation, contrary to Section 2 of the Fraud Act 2006 and one of Theft. The investigation found that he had made a series of fraudulent travel bookings between 15 March 2019 and 3 October 2019, to the total value of £30,018.33. He attended a voluntarily attended an interview under caution on 28 April 2021 and provided a 'no comment' interview. In his sentencing, having considered the character references, the judge described the fraudster as *"stupid"*, saying *"he has done it all to himself…"* and *"…he only stopped offending when he was caught."*

NATIONAL CASE: WESTMINSTER DENTIST SENTENCED FOR £74K FRAUD

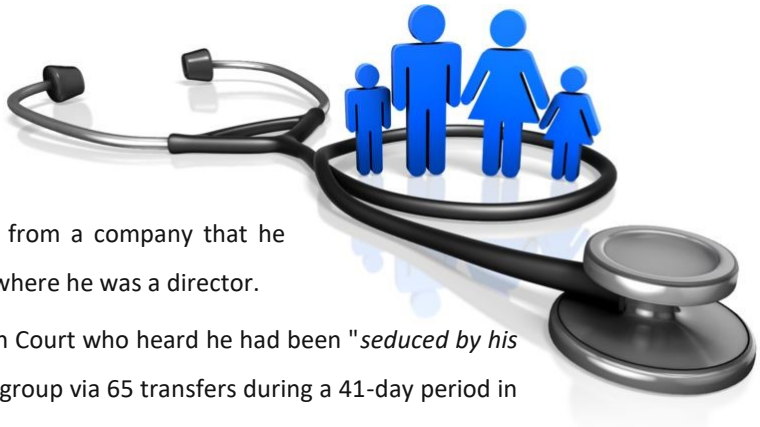


A fraudulent dentist who owned practices in London and Surrey has been sentenced today at Southwark Crown Court, following a fraud investigation led by the NHS Counter Fraud Authority (NHSCFA). The dentist, who had pleaded guilty to fraud by abuse of position at an earlier hearing, was sentenced to 20 months' imprisonment suspended for two years, ordered to carry out 250 hours of unpaid work, given a 20-day rehabilitation order and ordered to pay £662.00 of the NHSCFA costs within 3 months. The investigation started thanks to a call to the NHSCFA's fraud and corruption reporting line, run by Crimestoppers. The dentist held contracts with the NHS to provide dental services from two practices. When interviewed by NHS investigators, she argued that if she owed the NHS money it was only due to poor administrative practices, confused record-keeping but not dishonesty. However, this did not explain the scale of the problem. When the investigation compared payments data with patient records from one practice, it showed she had submitted 378 fraudulent claims over three financial years (April 2014 to March 2017) meaning she gained (and the NHS lost) over £74k that she was not entitled to. The majority of her false claims were for procedures that attracted the top rate of payment to a dentist from the NHS. The evidence indicated that she had carried out a calculated exercise to boost her revenue from the NHS with false claims and that it could not have happened through error. The dentist paid back the money shortly before sentencing, and only when the NHSCFA was about to start a confiscation investigation under the Proceeds of Crime Act. The payback figure was raised to £87,298.37 to account for inflation. Richard Rippin, Head of Operations at the NHSCFA, said: *"The great majority of dentists are skilled, honest, hardworking professionals who put their patients first. When [she] abused her trusted position by falsifying claims and claiming for work not done, she not only defrauded the NHS but let down the dental profession. It is quite possible that, had she not been caught, the scale of the debt and the crime would have increased exponentially."*

REGIONAL CASE: CHESTER-LE-STREET WOMAN STOLE £1.3M

A Chester-le-Street woman stole £1.3 million from Virgin Bank over a 6-year period in what has been described as a shocking abuse of trust. Her crimes were uncovered when someone standing in for her during a period of leave noticed a discrepancy. After being caught she tried to bluff police by saying she had only stolen £34,000. However, after a full internal audit, Virgin discovered that she had made 48 transactions to four accounts belonging to her, and one to a third party, totalling £1,309,719 between May 2013 and July 2019. The prosecutor said: "*She had transferred money to her own personal accounts then falsified records of the company to cover up what she was doing. So, on paper, everything reconciled but in reality, the shortfall had been paid to her various accounts.*" She had spent £42,000 on a new BMW, at least £26,000 on horses and equipment, £38,000 on PayPal debts and had also paid payday loan companies. The court heard the money had all gone but prosecutors have vowed to pursue her under the Proceeds of Crime Act. The 32-year-old, woman pleaded guilty to theft and transferring criminal property and was jailed for four years and nine months.

NATIONAL CASE: GP JAILED FOR FRAUD



A Portsmouth GP has been jailed for three years and four months after stealing £1.1 million during *"six weeks of madness"* to pay for his online gambling addiction. The 45-year-old GP stole the funds from a company that he founded, and which oversaw a group of GP practices in Portsmouth where he was a director.

He pleaded guilty to fraud by abuse of position at Portsmouth Crown Court who heard he had been "*seduced by his addiction to gambling*". The GP stole the funds from the healthcare group via 65 transfers during a 41-day period in 2020 to pay off slot machine and roulette debts. The court heard he gambled away £2.5m, of which he recouped £1.2m of his losses.

Government Counter Fraud Function

NHS

Beware of COVID Pass FRAUD

Criminals are using the NHS COVID Pass as a way to target the public by convincing them to hand over money, financial details and personal information. They are sending imitation text messages, emails and making phone calls pretending to be from the NHS, and offering fake vaccine certificates for sale online and through social media.

- **The NHS App is FREE**
- **The NHS COVID Pass is FREE**
- **The NHS will NEVER ask for payment or any financial details**
- **The NHS will NEVER issue fines or penalties relating to your NHS COVID Pass**

Do not respond to requests for money or important personal information such as bank details or passwords.

Be alert to links and attachments in unexpected text messages or emails.

The NHS COVID Pass is available to demonstrate your COVID-19 status either in a digital or paper format via the NHS App, the NHS website or by calling 119.

For information on how to get your FREE NHS COVID Pass visit

nhs.uk/NHSCovidPass

Further guidance and support

National Cyber Security Centre

If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to **report@phishing.gov.uk**. If you are suspicious about a text message, forward it to the number **7726**, which is free-of-charge.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by visiting **actionfraud.police.uk** or calling **0300 123 2040.**

CrimeStoppers.

If you have any information relating to NHS COVID Pass or vaccine certificate fraud you can stay 100% anonymous by contacting Crimestoppers online at **covidfraudhotline.org** or phone on **0800 587 5030**.

NATIONAL CASE: GP PRACTICE MANAGER ABUSED POSITION TO OBTAIN DRUGS

A GP practice manager has been dismissed and received a police conditional caution for falsifying prescriptions for 30mg codeine phosphate tablets between July and December 2017. The fraud came to light when the Data Analytics Learning Laboratory at the NHS Business Services Authority (NHSBSA) reviewed one patient's codeine prescribing which revealed that they appeared to have received 4,084 codeine phosphate tablets over that period (over twice the recommended dose). Further enquiries identified that the drugs had been prescribed from two GP practices (over 60 miles apart) and dispensed from six different pharmacies. Evidence gathered as part of the investigation found that the practice manager had created at least 125 false prescriptions and that between April 2015 and July 2020 they had obtained 27,236 codeine tablets and thousands more of other supplementary drugs. This deception caused a loss to the CCG's prescribing budgets through drug costs and dispensing fees totalling £3,110.20. Following the investigation, a decision was made to issue a formal police conditional caution, which the ex-practice manager accepted on 19 October 2021. The conditions imposed were that the individual was required to report any future work in the NHS, that they pay £500 compensation to the NHS body who suffered the loss and that they provide letters of apology to each of the GP practices that were affected.

SCAM ALERT:

Family members of online daters are being urged to help protect their relatives from becoming victims of romance fraud, as new figures show almost £92 million has been lost through dating scams this year alone. Daters who strike up online relationships between Christmas and Valentines Day tend to be the most susceptible to romance fraud, with a spike of 901 reports recorded by the National Fraud Intelligence Bureau (NFIB) in March 2021. Despite a peak of romance fraud reports and losses of £8.7 million reported in March, the financial spike came two months later in May 2021 where losses of a staggering £14.6 million were reported. Temporary Detective Chief Superintendent Matt Bradford, from the City of London Police, said: *"Typically, romance fraudsters will spend weeks gaining their victims' trust, feeding them fabricated stories about who they are and their lives - and initially make no suggestion of any desire to ask for any money, so the victim may believe their new love interest is genuine. But weeks, or sometimes months later, these criminals will ask for money for a variety of emotive reasons and as the emotional relationship has already been formed, victims often transfer money without a second thought. We're calling on family members who think their relatives may be dating online to help make them aware of the warning signs that they could be falling victim to fraud, particularly if the person dating online is not particularly tech savvy."* Criminals often use a range of stories to get victims to transfer them money without it raising suspicion. The stories are often believable, to a certain extent, and something that the victim would find hard to say no to, especially because of their emotional attachment. Examples of stories include funding travel to visit the victim, money to pay for emergency medical expenses, lucrative investment opportunities and pretending to be military personnel or working overseas.

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at police.uk or by calling 0300 123 2040.

MEET THE COUNTER FRAUD TEAM

Terry Smith

Director of Operations

T: 07971895281

E: terry.smith@audit-one.co.uk

Rebecca Napper

Head of Operations (Proactive)

T: 07980726508

E: rebecca.napper@audit-one.co.uk

Michelle Watson

Head of Operations (Reactive)

T: 07580589024

E: michelle.watson@audit-one.co.uk

Paul Bevan

Counter Fraud Specialist

T: 07973814286

E: paul.bevan@audit-one.co.uk

Gemma Collin

Counter Fraud Support

T: 07920590180

E: gemma.collin@audit-one.co.uk

Martyn Tait

Counter Fraud Specialist

T: 07976433667

E: martyn.tait@audit-one.co.uk

Iain Flinn

Counter Fraud Specialist

T: 07973814207

E: iain.flinn@audit-one.co.uk

Stephen Veitch

Counter Fraud Specialist

T: 07973814475

E: stephen.veitch@audit-one.co.uk

Kathryn Wilson

Counter Fraud Specialist

T: 07973814205

E: kathryn.wilson@audit-one.co.uk

Simon Clarkson

Counter Fraud Specialist

T: 07980729654

E: simon.clarkson@audit-one.co.uk

David Wearmouth

Lead Investigation Officer

T: 07919545248

E: david.wearmouth@audit-one.co.uk

Gary Ross

Security Management Specialist

E: gary.ross@audit-one.co.uk

Paula Temperley

Investigator

E: paula.temperley@audit-one.co.uk

Tracey Moore

Investigator

E: tracey.moore1@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060