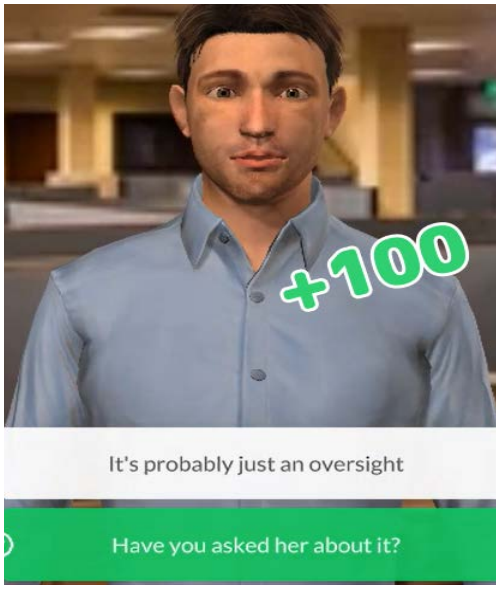
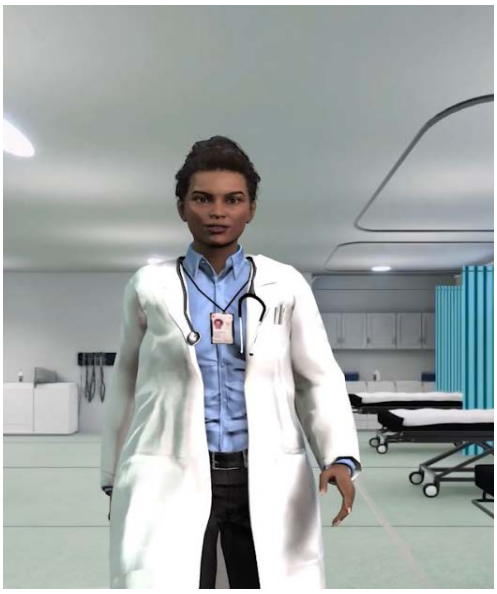
# Talking Fraud

Spring 2023



## Liverpool University Hospitals & MIAA launch 'game-changer' tech to clamp down on fraud

MIAA, working with our host Trust, Liverpool University Hospitals NHS Foundation Trust (LUFHT) launched a cutting-edge training initiative to combat fraud and improve financial management across the NHS. To prevent fraud and money mismanagement across the NHS, LUHFT and MIAA have partnered with Attensi, the leading game-based training specialist, to create off-the-shelf financial training for Trusts across the country. Together, they are aiming to improve staff knowledge of best practices for a range of financial topics, including reporting and identifying fraud, audit readiness and budget management.

Darrell Davies, MIAA's Head of Anti-Fraud Services, said: *"Attensi's game-based training aims to increase NHS staff's vigilance to possible wrongdoing and improve their awareness of the appropriate channels to report their concerns. MIAA is proud to have been involved in the development of this innovative training which supports our fraud and assurance teams in sharing and reinforcing key messages on what is rightly a highly important issue for anyone working in the NHS. Partnering with Attensi has revolutionised the way in which we deliver training. The convenient and digestible way in which the training is delivered has boosted engagement and fits easily around the busy schedules of NHS staff."*

The app is designed with psychology and repetition at its core, and the innovative tech-driven approach to learning gives users a unique training experience. The enjoyable and stimulating game-style training improves retention rates by encouraging repeat attempts.

Jonathan Moffett, Global Sales Enablement Director and NHS Lead for Attensi, said: "*Being given the opportunity to partner with the NHS to create training that will help the organisation provide an even better service is a privilege.*"

In this edition:



Pictured: Screen shots from the training game

# News

## “How can I protect myself online?”

Having strong social media security is essential. This video covers important NCSC guidance which will allow for robust cyber security for your online devices and data!

It covers how to keep your accounts secure, including setting a strong password and 2 step verification, and how to deal with compromised accounts.

Watch here or visit WM Regional Cyber Crime Unit YouTube Channel.



## Fraud reclassified as national security threat

The UK government has announced that fraud will be reclassified as a national security threat, giving it the same status as terrorism. Additionally, fraud will be added to the Strategic Policing Requirement, this means it will be treated as a top priority alongside public disorder, serious and organized crime, civil emergencies, cyber-attacks, and child sexual abuse. The reclassification follows the 2022 Annual Report on Suspicious Activity Reports (SARs) by the National Crime Agency (NCA). Published in January 2023, this report highlights that the past two years have been dominated by organized crime threats, particularly fraud, against members of the public, UK businesses, and government departments.

Fraud is the most commonly experienced crime, estimated to account for 40 percent of all crimes committed across the country. In 2022, total losses amounted to £4 billion, a 67 percent increase from 2021. Despite these figures, fraud teams account for 2 percent of police resources and the number of prosecutions represents 0.75 percent of reported fraud cases.

Cheque, card, and online banking are the most reported type of fraud by volume, according to the most recent UK National Risk Assessment (NRA) with cybercrime a major enabler of fraud. The proportion of fraud incidents that were cyber-related in the year ending March 2022 increased to 61 percent.

A key part of the government’s overhaul regarding fraud includes the replacement of the national reporting service Action Fraud, following criticisms of its performance. The replacement service is intended to more seamlessly integrate into the current fraud landscape, sharing data with the National Cyber Security Centre (NCSC) and the National Economic Crime Centre (NECC), both of which have been created since Action Fraud was launched. The government also hopes to improve automation in the service, allowing more timely sharing of information.

# Recent Cases

## Jail for woman who landed senior NHS post with bogus CV


A woman who cheated her way into a top NHS post with lies on her CV and bogus references has been jailed for 12 months.

Chanelle Poku, 29, pretended she had a Master's degree in molecular biology and experience leading a charity to land a senior job with NHS Croydon's Clinical Commissioning Group.

She was put in charge of delivering programmes for urgent care patients in the borough, and when challenged over her failing performance, she made a string of false accusations of bullying, assault and racism.

Poku, who even sent a bogus letter from a lawyer to the NHS to try to derail the investigation into her conduct, was found guilty by a jury of fraud by false representation. "This was a role of some responsibility and you plainly didn't have the skills for it", said Recorder David Osborne, sentencing Poku to 12 months.

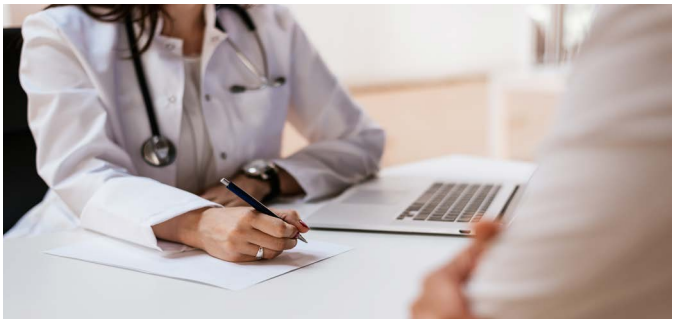
"Your offending left a wholly-unqualified person in charge of an important role in the local NHS infrastructure. This offence is so serious that only an immediate custody is justified."

Poku, who lives in Westminster, earned £13,171 before she was suspended. At trial she tried to blame a recruitment agency for the lies on her application form. Poku, who has been in custody since the verdict in July, now claims to have accepted her guilt and has offered to repay the NHS body her wages.

## Camberwell preacher sentenced for selling £91 'plague kit' to cure COVID

A London preacher who sold a "plague protection kit" to guard against COVID has been given a suspended jail sentence and ordered to pay £60,000. Bishop Climate Wiseman, 47, was convicted of fraud after selling the package made up of an oil mixture and scarlet yarn. A jury found him guilty in December, and a judge at Inner London Crown Court has now passed sentence. Wiseman's one-year prison term is suspended for two years. He was also told to do 130 hours' community work.

## Fake Doctor sentenced to seven years for fraud and forgery



A woman who forged her medical qualifications to obtain senior positions within the NHS as a hospital psychiatrist has been sentenced to seven years imprisonment at Manchester Crown Court after being found guilty of 20 offences including fraud and forgery.

In an investigation led by Cumbria Police and supported by the NHS Counter Fraud Authority, Zholia Alemi was found to have fraudulently obtained in excess of £1million from the NHS during the twenty-two years that she worked within a number of UK health bodies posing as a qualified psychiatrist.

Richard Rippin, Head of Operations at the NHS Counter Fraud Authority said: "Zholia Alemi has deceived the NHS over a considerable period of time and practised under forged and false qualifications, with the potential for harm to patients. This outcome and sentence is warmly welcomed as a suitable punishment for this appalling deception, as well as an acknowledgement of the substantial amount of NHS money she has fraudulently obtained during the period of employment, which we will now take steps to recover."

# Preventing ID & CV fraud
## Learning from the Alemi Case

Kevin Howells, Anti-Fraud Manager

It has been in the news recently that Zholia Alemi, who had faked a medical degree certificate from New Zealand 25 years ago to work as a psychiatrist for more than two decades in the NHS in the UK, has been jailed for seven years for 13 fraud offences, amongst other offences.

Zholia Alemi worked across the UK after claiming to have qualified at the University of Auckland, but how could this have happened? She had started her medical studies but had not completed them. She provided a forged medical certificate and a verification letter, which included a misspelling of “verify”.

ID checks and Right to Work checks are undertaken on all new starters to the NHS, and this has been the case for many years. It is a comprehensive system where the applicant has to provide a combination of proof of ID and proof of address documents (passport / Birth Certificate / Residence Permit / Utility Bill / HMRC letter etc). This process does not include any check on qualifications, but qualification certificates are still verified by the Recruitment team.

According to the latest NHS workforce statistics, there are more than 1.2 million Full Time Equivalent (FTE) staff currently working in the NHS. Professionally qualified clinical staff (Doctors, Nurses and Allied professionals) make up over half of these FTE roles (52.9%) and their governing bodies (General Medical Council, The Nursing & Midwifery Council, and The Health and Care Professionals Council) provide services where NHS organisations check with the Governing Body whether an applicant in these areas is qualified (and not disqualified).

The GMC have already admitted failings in their historic system in relation to Zholia Alemia, and instigated further checks on 2,500 other historic foreign doctors working within the NHS; but what about non-clinical roles? According to those earlier statistics there are in excess of 500,000 non-clinical staff currently working in the NHS, and many of those will be qualified, whether that be in Accounting, IT, Secretarial skills, Procurement or a broad range of other areas, including Accredited Counter Fraud Specialists.

We provide Right to Work / Employment Check training for our clients (half or full day versions), and in a session a few years ago we had a discussion about how the Recruitment Team would check the qualifications of an IT professional applicant if the qualification certificate was in Arabic. The answer was that they would get the applicant to translate it for them, not quite the answer we were expecting!

My point is that if, say, a Doctor has been working for the same NHS organisation for 25+ years, the checks on their application process then were not as stringent as they would be now, in terms of ID or qualifications, and there is the possibility that they may not be who they say they are, and may not be a qualified Doctor. Perhaps there should be periodic re-reviews of qualifications as/when people progress through an organisation (i.e. stay with the same employer for years). A subsequent check might pick up something that was missed in a previous check.

Similarly, robust systems for checking qualifications for non-clinical roles should also be reviewed. There are paid-for services that can verify degree qualifications in the UK, but are there always fool-proof verification systems for unusual qualifications, those that are not often seen? If I provided my original Accredited Counter Fraud Qualification certificate, would someone in Recruitment know what to look for and whether is it genuine?

# New Legislation - Economic Crime Corporate Transparency Bill

The Government is proposing new legislation that has several aims, amongst which is to prevent fraudsters "using companies and other corporate entities to abuse the UK's open economy." Anti-corruption group Transparency International claimed in 2017 that hundreds of UK companies were implicated in nearly £80 billion of money laundering. The Government accept themselves that aspects of the UK's company regime have made it particularly attractive to criminals, including fraudsters, who might want to use corporate structures to hide wealth or enable money laundering.

The UK ranks joint 18th on Transparency International Corruption Perceptions Nation Index in 2022, behind Uruguay, Hong Kong and Estonia amongst others. In 2016, before the Brexit vote, it was Joint 10th.

Part of the Bill relates to Companies House reform. It is currently simple to set up a limited company in the UK, it can take less than 24 hours and cost £12 (compared to more than £250 on the continent). Companies House itself is not a regulator, more of a processor of filed documents, and cannot query or investigate any of the documents that are filed there. Fraudsters could also use information on the Companies House register to impersonate others, or register companies with incorrect information (such as false addresses).

At the present time a company structure could be such that a 100% shareholder of Company A could be Company B, and vice versa, clearly a nonsense. Companies House agree this is not useful or transparent, but they can do nothing to prevent this sort of obfuscation.

Clause 28 of the Bill aims to deal with address fraud as it intends to require companies to ensure their registered office address is "appropriate", meaning somewhere that documents delivered to it can be acknowledged, and would be expected to come to its attention. This used to be a Solicitor's address if the company did not have their own trading address. In the future, a failure to give an appropriate address would be a criminal offence committed by the company and every responsible officer.

Clause 52 intends to update the filing requirements for micro-entities and limited partnerships to require them to file a balance sheet, a profit and loss and a directors' report. At present "small" companies do not need to file accounts, meaning there is often very little available information at Companies House on the majority of entities, other than lists of Directors and shareholders. This reduced disclosure requirement makes the UK attractive to fraudsters who wish to present a false picture to others.

Clause 148 aims to make it easier for businesses and professional advisers in the regulated sector to share data, for example, where one business wants to warn another business about the risk of economic crime of a customer. This easing of restrictions would also apply to indirect disclosures made via a third-party intermediary, such as the National Fraud Database.

Finally, the Serious Fraud Office powers would be extended such that the Director of the Serious Fraud Office's pre-investigations would no longer be restricted to cases involving only international bribery and corruption.

# 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 straight-forward, 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
Senior Anti-Fraud Manager
07552 253068
Paul.Bell@miaa.nhs.uk

Claire Smallman
Senior Anti-Fraud Manager
07769 304145
Claire.Smallman@miaa.nhs.uk

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

Ruth Barker
Anti-Fraud Specialist
07584 774 763
Ruth.Barker@miaa.nhs.uk

Alun Gordon
Lead Counter-Fraud Specialist
07469 573 678
Alun.Gordon@miaa.nhs.uk

Kevin Howells
Anti-Fraud Manager
078257 32629
Kevin.Howells@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
07584774761
Paul.McGrath@miaa.nhs.uk

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

Michelle Moss
Anti-Fraud Specialist
07825 858685
Michelle.Moss@miaa.nhs.uk

Andrew Wade
Anti-Fraud Specialist
07824 104 209
Andrew.Wade@miaa.nhs.uk