

## Hospital consultant sentenced after forging timesheets

A hospital consultant and high-profile social media influencer has been sentenced to 24 months suspended thanks to the work of NHS counter fraud professionals.

Dr Kifayat Ullah pleaded guilty in December to defrauding the NHS of more than £50K by submitting false timesheets during his time as a locum at Kingston Hospital NHS Foundation Trust.

Local Counter Fraud Specialists and the NHS Counter Fraud Authority Fraud Hub worked together to fully uncover the extent of Dr Ullah's offending following an audit at the Trust identifying discrepancies within records presented. After extensive investigations revealed the full scale of the dishonesty, the Crown Prosecution Service agreed that the evidence available warranted a charge of making a false instrument with intent it be accepted as genuine under the Forgery and Counterfeiting Act 1981.

At sentencing the Judge His Honour Trigilgas-Davey said: "His actions stem from greed, he has brought disgrace on himself and his profession."

Dr Ullah was recruited as a locum consultant to help with post-covid backlog within the Trust. He almost immediately asked to reduce his hours to part-time working.

However, for six months, he submitted 29 forged timesheets to his agency purporting that he was working full time and was paid accordingly. Some timesheets were altered after genuine authorising signature, others he just made up himself and forged or copied signatures.

NHSCFA Head of Operations Richard Rippin said: "We are delighted with the sentence given out, and I commend the action taken by Kingston Hospital. This was a blatant abuse of Dr Ullah's position of trust and a deliberate attempt to take, for his own personal gain, NHS money intended for the provision of patient care."

"This action demonstrates the value and impact of the local counter fraud response working across the NHS to identify and pursue offenders like this and protect NHS funds from this type of deliberate fraud."

In this edition:

Hospital consultant sentenced after forging timesheets

Talking Fraud podcast new episodes released

Travel smartcard scam

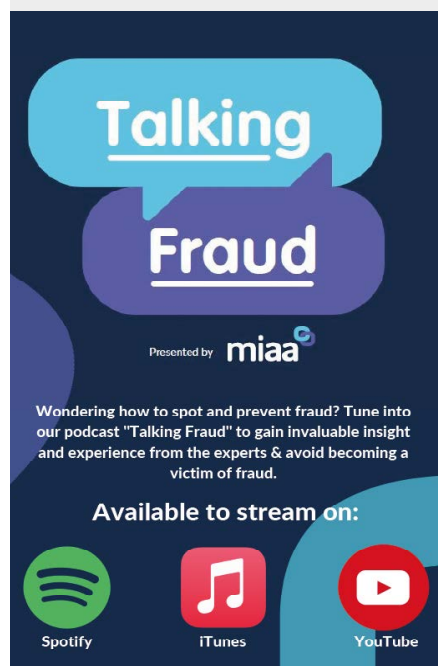
Sympathy for fraudsters

How mandate fraud is linked to romance fraud

Consequences of fraud

Useful sources of information

MIAA Anti-Fraud Team contact details



**Talking Fraud**

Presented by **miaa**

Wondering how to spot and prevent fraud? Tune into our podcast "Talking Fraud" to gain invaluable insight and experience from the experts & avoid becoming a victim of fraud.

Available to stream on:

Spotify iTunes YouTube



# News

## New episodes of Talking Fraud released!



The latest two episodes of the MIAA fraud podcast, Talking Fraud are being released in February and March.

Designed to provide a light-hearted and informative view of fraud in the NHS and also the wider issues that can impact us all.

Paul Bell, MIAA's Senior Anti-Fraud Manager said: *"We've had a great response to the podcasts. They are a great way to get the anti-fraud message out there. I'd encourage all of you to share them with your colleagues."*

Episode four covers social engineering and fraud, outlining this technique so that you can identify it and protect yourself.

In episode five our team dives into conflicts of interest in the NHS, comparing UK regulations with global standards and looking at the impact on the NHS.

*"I'd encourage all of you to share them with your colleagues."*



You can download the podcast from Spotify, Apple Music and all streaming platforms or via this QR code.

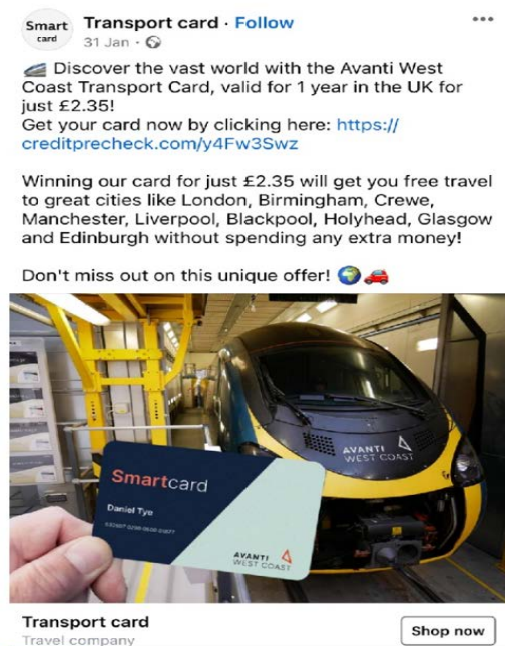
## Avanti Travel Smartcard Scam



by Andrew Wade

MIAA has been alerted to a new scam in which free travel is offered on Avanti West Coast Trains if you purchase a surprisingly cheap transport card from them.

The fraud starts with Avanti West Coast appearing to offer a giveaway on social media, with UK residents seemingly able to "win" a smart card for travelling with them for one year for only £2.35. Clicking on the provided website link will direct you to a web page where you will be asked to play a game before being asked for your bank details to pay for the card at this seemingly great value amount.



Having "won" the card you are then promised free travel to great UK cities without spending any extra money for a whole year. Avanti West Coast have confirmed that there is no such travel card provided by the company at this rate, and nor do they offer free travel to UK cities.

Individuals should not click on any weblink nor should they provide any personal information or bank details, unless they are sure of the authenticity of any website. Click on the following link to report any such fraud or scam on the [Action Fraud website](#).

Always remember the adage: if something looks too good to be true, that's because it usually is!!



# Sympathy for Fraudsters

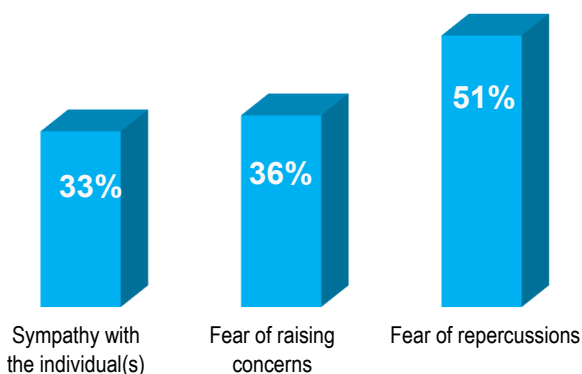
by Kevin Howells



On a periodic basis, MIAA conducts fraud, bribery and corruption staff surveys at our clients. This is partly to show evidence of meeting a fraud standard, and prove we are carrying out our “understand” activities (The Strategic Pillars | NHSCFA Strategy 2023-26 | NHS Counter Fraud Authority) to the NHS Counter Fraud Authority.

Typically, we do not always get a great level of response, but the responses we do get provide a wealth of useful information, not only in providing feedback on the information we produce – and which gets promoted at the NHS organisation – but also on the opinions and knowledge of NHS staff about fraud and, crucially, how they would respond should they identify a fraud.

What we, as counter fraud professionals, would like to see, is that 100% of survey respondents would report instances of fraud, and report it to us, the Anti-Fraud Specialists, but that is sadly never the case. In the 2021/22 Fraud Staff Surveys at one Trust, the responses to the question “*What do you think may prevent you from reporting any suspicion of fraud, bribery and/or corruption that was happening at work?*” threw up some interesting answers, including the following:



2) and 3) are dealt with quite easily, in that there is legislation in place to protect those raising concerns [The Public Interest Disclosure Act 1998 (PIDA) provides legal protection to workers “blowing the whistle”], and no-one should be penalised for raising a genuine concern such as a potential fraud (unless it is malicious), though we understand why NHS staff may be reluctant to blow the whistle given the experience of those that did just that in the Lucy Letby case (admittedly not a fraud case). Also, the NHS Counter Fraud Authority enables concerns to be raised anonymously anyway, if needs be, by a confidential telephone line **0800 028 4060** or by filling in a form on their website <https://cfa.nhs.uk/reportfraud>.

For 1) this response was higher than in previous years, and related to a third of all Trust staff. When someone identifies a



suspected instance of fraud in any organisation, I expect they first put themselves in the shoes of the alleged perpetrator and think “*that could be me*”. We are in the midst of a cost-of-living crisis with spiralling fuel and food prices. It seems eminently reasonable for someone to think it is somehow morally wrong to report a hard-pressed Band 3 Healthcare Assistant, for example, and therefore understandable that they may not be keen on reporting them to their Anti-Fraud Specialist. The situation may be different if the fraudster were a medic or senior manager.

Remember though, if your clinical area is swamped, and management can’t provide more resources, the reason may be that fraudsters have taken some of the money that should be funding your department. Money lost to fraud at a Trust has a direct effect on the funding of the wards and departments at the Trust. More than a £1.26 billion pounds each year is lost to fraud in the NHS every year.





# How mandate fraud is linked to romance fraud



by Paul Kay



During my time investigating fraud for the Merseyside Police, it became clear that fraudsters do not just target one fraud type but will target multiple different types of fraud at any one time. Some of these frauds will overlap and assist the fraudster(s) when trying to launder their ill-gotten gains. Two such linked fraud offences that I noticed were mandate fraud and romance fraud.

A bank mandate is a set of instructions, which will include bank account details, and is used by people in a business such as the finance department, to pay suppliers.

Within a mandate fraud, the fraudster will target a supplier, either hack into their emails or create a bogus email that looks legitimate, and send their customers an email, requesting their bank account details have changed. The intention is that the customer takes this email at face value, and simply changes the bank mandate instructions, namely the bank account. The next time an invoice is paid by the customer, it will be credited to the new, fraudster controlled, bank account.

What I noticed in my time in the Police is that the fraudsters will often not supply their own bank account in these instances, as they do not want to be traced and identified, so will look to use another bank account under their control, but not traceable to them.

As such, the fraudsters may look to identify a bank account they

can use to launder the monies they receive from any successful mandate fraud they perpetrate. It is here that victims of the romance fraud can become involved, as their bank account is not linked to the fraudster, and therefore the fraudster cannot be identified should this bank account be investigated by the Police.

The romance fraud victim becomes involved at the request of the person they believe they are in a relationship with (the fraudster) and unknowingly they allow their bank account to be used to launder the monies from the mandate fraud to their own personal bank account, without realising that this is what is taking place.

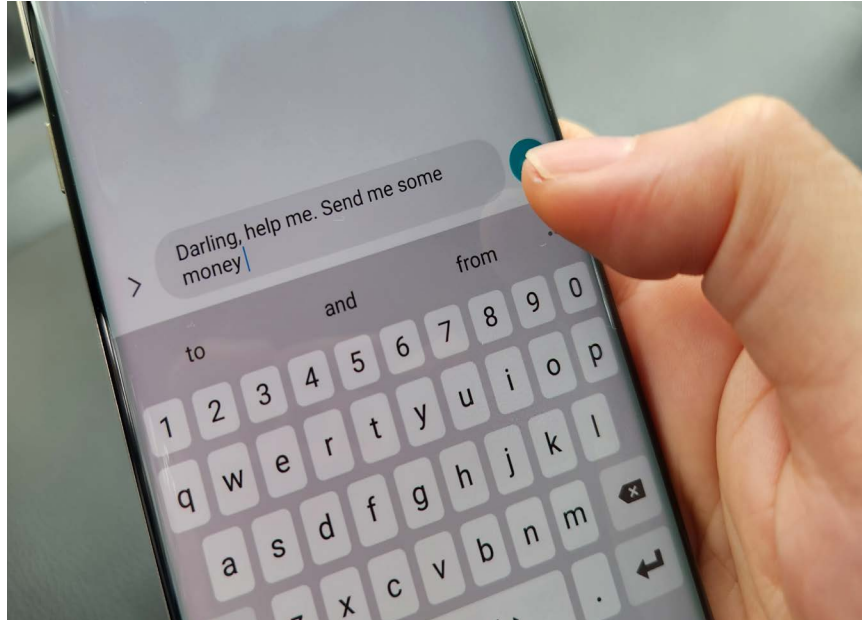
A fraudster will usually meet a romance fraud victim on a dating website, and they will then purport to work/or have a business overseas. Once they have got to know/established rapport with the romance fraud victim over several weeks of contact, the fraudster will claim to have short term money problems, claiming their bank account has been frozen for reasons unknown or not explained.

This will usually result in the romance fraud victim lending the fraudster monies on a short-term basis, so their fictitious business can continue to run by providing the fraudster with their bank account details. Unknown to the romance fraud victim, the fraudster may also be committing mandate fraud, whereby they supply the potential company/business victim with the romance fraud victim's bank details as part of the mandate fraud.



# How mandate fraud is linked to romance fraud

The fraudster will then tell the romance fraud victim that they (the victim) will be receiving a large sum of money into their bank account, as their (the fraudster) bank account is still frozen. They (the fraudster) will request that once the monies have been credited to their (the victim) bank account, they (the victim) forward these monies onto them (the fraudster) via a given method (often involving crypto-currency).



been online dating and embarrassed about their personal financial loss, which can be in the hundreds of thousands of pounds. Added to this, there is the emotional trauma caused to the romance fraud victim by the fraudster.

In some cases, the fraudster may tell the romance fraud victim to keep some of the monies credited to their account, depending on whether the victim had already lent the fraudster monies as part of the original romance fraud. This supports the romance fraud victim's belief that the transaction and intentions of the fraudster are genuine, but what they don't realise is that they have unwittingly enabled the laundering of monies for the fraudster using their own bank account and committed a crime.

Several weeks may pass but eventually the romance fraud victim may have their bank account frozen or be contacted by their bank/police and be asked to explain why their account has been used for fraudulent purposes.

Even if they are eventually cleared of any wrongdoing - and this may take an extended period of time - during this period the victim's own bank account may still be frozen by either their bank or the police, causing the account holder financial difficulties in addition to emotional distress. In some cases, the innocent account holder may have their home address searched, assets seized and be arrested, or interviewed under caution.

In some other cases, the romance fraud victim will end up not reporting their involvement to the police, due to embarrassment and not wanting other family members to know they had

There are red flags to look out for to see if you are the victim of romance fraud:

- They refuse to video call.
- They refuse to meet in real life.
- They are too good looking.
- They try to move conversations off the platform where you initially meet.
- They declare their love quickly.
- They claim to be working overseas.
- When they ask for money, it will be time-critical, and for a reason you can't help wanting to help (both social engineering tricks)
- They ask you to keep "the relationship" secret.

Find out more about [romance fraud from Crimestoppers](#).

**If you have been a victim of fraud or cybercrime, report it at [www.actionfraud.police.uk](http://www.actionfraud.police.uk) or by calling 0300 123 2040.**

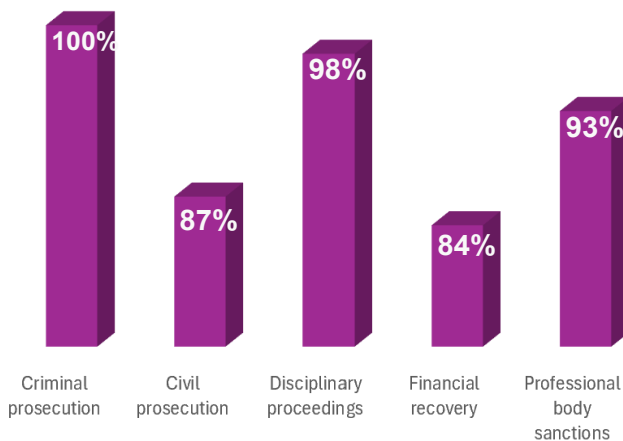


# Consequences of Fraud



by Kevin Howells

On a recent Fraud Staff Survey for a client, I was delighted to see that 100% of respondents knew that one of the consequences of committing fraud was a criminal prosecution, and we already focus on that in fraud awareness sessions.



There was good awareness shown of some of the other consequences, but the response rates could have been better; so here is some more detail on those non-criminal consequences, as a refresher.

Whenever we, as Anti-Fraud Specialists, receive a fraud referral, we judge whether there has been a fraud offence committed, and then work to see whether there is enough evidence to justify a criminal prosecution. This isn't always the case. For the criminal case we must prove "beyond reasonable doubt" that the offence was committed, which means if there is any doubt about the quality of the evidence we have obtained, the case will be rejected by the Crown Prosecution Service

But there are other consequences as well, and the first of those are disciplinary proceedings, if the subject is an NHS employee. For disciplinary proceedings to take place, the burden of proof is different and of a lower nature than for a criminal case, i.e., it is easier to prove. The offence must be proven on "the balance of probabilities". If a fraud has been committed by a staff member, then this is likely to be considered gross misconduct, and the consequence of gross misconduct could be the termination of employment.

If the person who has committed fraud has been prosecuted (criminal prosecution) and dismissed (disciplinary proceedings), then there are still potentially more consequences. If the

fraudster works as part of a regulated profession (such as Doctors - GMC, Nurses - NMC, Radiologists - HCPC, Pharmacists - GPhC and there are more) then the regulatory body may commence proceedings and the fraudster may receive Professional Body sanctions. They may be barred from working in their chosen field, or even banned for life, [like this Doctor](#).

Beyond that, there are still more consequences, of a financial kind. Did you know that if a fraud has been proven, you are nearly always asked to repay the fraudulent payment? If you have claimed 100 hours of overtime at £25, and after you have been prosecuted, dismissed from your job and banned from



working in your chosen profession (and even if none of those things happen), you then have to pay back the fraud amount (financial recovery), [like these fraudsters](#).

If you refuse to pay back the fraud money, and if the overpayment has been identified while you are still employed, this may be held back from your salary. If you have been dismissed or have resigned, then your employer has grounds to apply for a Court Order to get the fraud money back from your NHS pension. Can you imagine having to explain to your significant other, that as well as being prosecuted for fraud (and potentially spending time in prison), losing your job, and losing the right to work in your chosen profession you are also having to pay back the proven fraud amount from your intended retirement fund?

In addition to all of that, if your fraudulent act has caused a significant loss to the organisation, you may also be sued by the Trust for reputational or other damages (civil prosecution).

# 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

Belinda Corris  
Anti-Fraud Specialist  
☎ 07570 146911  
✉ Belinda.Corris@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