



MIAA Fraud team launch 'Talking Fraud' Podcast

The MIAA fraud team have launched their latest product, a fraud podcast. Designed to provide a light-hearted and informative view of fraud in the NHS and also the wider issues that can impact us all.

Darrell Davies, MIAA's Regional Assurance Director (Anti-Fraud) said: *"There are so many anti-fraud messages to get out there. We are always looking for innovative ways to engage with our audience and creating a series of podcasts seems like a great opportunity to do this."*

MIAA's anti-fraud team have many years of experience in investigating fraud across a range of organisations. Darrell is joined by his colleagues, senior anti-fraud managers, Paul Bell, Claire Smallman and Anti-Fraud Manager, Kevin Howells to discuss all aspects of fraud and fraud prevention.

Darrell continued: *"Fraud can be committed by anyone, from patients who should be paying for their prescribed drugs; to staff and contractors who have submitted timesheets or invoices for work that they haven't done; to external fraudsters who attempt to commit bank mandate fraud by pretending to be a genuine supplier and then deceive the NHS organisation into paying invoices into an account controlled by the fraudster."*

The first Episode, "NHS Fraud – what's the problem?", examines how the NHS Counter Fraud function came into place and what the current NHS counter-fraud situation looks like now with Covid-related and cyber enabled fraud becoming more prevalent.

Future episodes look at the work of the anti-fraud team and the learning from a few interesting cases, looking at the methods and motivations of fraudsters and the outcomes for them when they are caught.

You can download the podcast from Spotify, Apple Music and all streaming platforms.

In this edition:

Talking Fraud Podcast Launch
NHS CFA Strategy 2023-26 and Business Plan 2023-24

International Fraud Awareness Week

Government Fraud Strategy

New Fraud Legislation

Cyber Savvy Campaign

Spot the signs of fraud in your workplace

AI Fraud Risks

WhatsApp Scam Warning

Useful Sources of Information

MIAA Anti-Fraud Team contact details





International Fraud Awareness Week starts on 13 November 2023



The annual global campaign to minimise the impact of fraud by promoting anti-fraud awareness and education takes place between 13 to 19 November 2023. We'll be supporting this with a campaign which will be rolled out to all our clients. Keep an eye out for key messages that week!

Government Fraud Strategy

In May 2023, the Home Office presented a Fraud Strategy to Parliament, entitled "Fraud Strategy: Stopping Scams and Protecting the Public".

The Home Secretary's Foreword to this document summarises the intention of the Strategy, noting the harm fraud causes to the economy and people's lives, and that it funds other serious crimes. It talks about the Government not tolerating "the barrage of scam texts, phone calls, adverts, and emails that causes misery to millions", and points out that fraud makes up more than 40% of all crime, but "receives less than 1% of police resource".



NHSCFA Strategy 2023-26 and Business Plan 2023-24 launch

The [new strategy and business plan](#) sets out the key priorities to counter fraud in the NHS over the next three years and outlines how the NHS Counter Fraud Authority intend to work collaboratively with the health sector to understand, find, and prevent fraud in the NHS.



Following an extensive program of collaboration, feedback, and input from a wide range of key partners, the focus will be on four strategic pillars of activity - Understand, Prevent, Respond, and Assure - that will form the basis of everything NHSCFA does. At the heart of this new approach is their new vision which will build upon our partnership working.

NHSCFA's CEO, Alex Rothwell, said: "I am committed to strengthening our collaboration and engagement with key partners ... Data analytics and insight will be at the heart of our approach. The creation of a new Fraud Hub will also herald a new approach to support and enable alignment between the national and local counter fraud response and cut across all four pillars of the strategy, generating a joined-up approach to tackling fraud, bribery and corruption within the NHS".



Protect yourself online

This year, Cyber Security Awareness Month runs from Sunday 1st to Tuesday 31st October 2023. To support this, the Cyber Savvy Month campaign will be taking place across Cheshire and Merseyside. The resources and information on the cyber savvy website are useful to everyone as it offers advice and guidance on keeping yourself safe with advice on updating passwords, software, multi-factor authentication and recognising and reporting phishing attacks. Check out: [be-cybersavvy.co.uk](https://www.be-cybersavvy.co.uk)



Government Fraud Strategy

Continued from page 2

The strategy includes proposals for 400 new specialist investigators for Police in England and Wales in a new National Fraud Squad, replacing Action Fraud, and creating powers to “make sure that payment service providers are treating customers fairly”. More than that, the strategy asks business sectors, including online technology giants, to go further to protect customers, citizens and businesses, in association with the Online Safety Bill. The intention is to provide information on which platforms are the safest.

The strategy makes reference to working will allies abroad, hosting a summit of international partners, and appointing a Prime Minister’s Anti-Fraud Champion (Conservative MP, Anthony Browne.)



Browne

As well as the above, specific targets include:

- Cut fraud by 10% from pre-2019 pre-covid levels
- Ban cold calls
- Ban SIM farms
- Review the use of text aggregators.
- Making it harder to “spoof” UK phone numbers
- Stop people hiding behind fake companies
- Take down fraudulent websites
- Replace Action Fraud with a new system for reporting fraud and cyber crimes to the Police
- Change the law so that more victims of fraud will get their money back
- Make it easier to report fraud to technology giants
- Imprison more fraudsters
- Introduce a new Failure to Prevent Fraud offence in the Economic Crime and Corporate Transparency Bill
- Recruiting 1,000 new judges and increasing judicial capacity
- Recruit 2,000 new Magistrates by 2025
- Increasing the number of Fraud Act 2006 cases that can be heard at Magistrates Court
- Overhaul public anti-fraud communications

It should be noted that rarely do any of the claims in the strategy include any sort of timescale for their implementation, though £100million of investment in law enforcement is included in 2024/25 and committed £30 million across three years to replace Action Fraud, and the replacement service “will launch within a year”.

New Fraud Legislation could impact NHS

Did you know that fraud makes up 41% of national crime? It is no wonder the current Government is proposing new fraud legislation.

The existing fraud legislation, the Fraud Act 2006, has not been amended since, making clear the fraud offences that can be committed by individuals:

- Section 2 – Fraud by false representation
- Section 3 – Fraud by failing to disclose information
- Section 4 – Fraud by abuse of position

Unlike the Bribery Act 2010, there is no offence of “failing to prevent” fraud contained in the Fraud Act 2006, and this is what the Government is proposing.

Under the new offence, “an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation’s benefit”, and the organisation does not have “reasonable fraud prevention procedures in place”. The intention is that this can apply whether the company bosses ordered or knew about the fraud, or not.

There are financial limits to show for which organisations the new offence will apply, but this will include all NHS bodies. Organisations will be able to avoid prosecution “if they have reasonable procedures in place to prevent fraud”. Further guidance is expected from the Government if and when this new legislation comes into force.

It is the organisation that will be punished in this proposed legislation, and not individuals, and the organisations can receive an “unlimited fine”.

The Counter Fraud measures in place at NHS bodies are in a good position to be ready for this new fraud offence. By employing an Anti-Fraud Specialist, either directly, or via organisations like MIAA, NHS bodies have a raft of policies and procedures in place to evidence having “reasonable procedures” in place for fraud prevention, including:

- Anti-Fraud, Bribery and Corruption Policy
- Fraud Risk Assessments
- Anti-Fraud Work Plan
- Mandatory Training
- Fraud Awareness Activities
- Local Proactive Exercises
- National Fraud Initiative

We will keep you updated on whether this new legislation comes into being.



Could you spot fraud in your workplace?

BEHAVIORAL RED FLAGS OF FRAUD

Recognising the behavioral clues displayed by fraudsters can help organisations more effectively detect fraud and minimise their losses.

8 KEY WARNING SIGNS

85% OF ALL FRAUDSTERS displayed at least one **BEHAVIORAL RED FLAG**

These are the 8 most common behavioral clues of occupational fraud. **At least one of these red flags** was observed in 76% of all cases.



39%

Living beyond means



25%

Financial difficulties



20%

Unusually close association with vendor/customer



13%

Control issues, unwillingness to share duties



12%

Irritability, suspiciousness, or defensiveness



12%

Bullying or intimidation



11%

Divorce/family problems



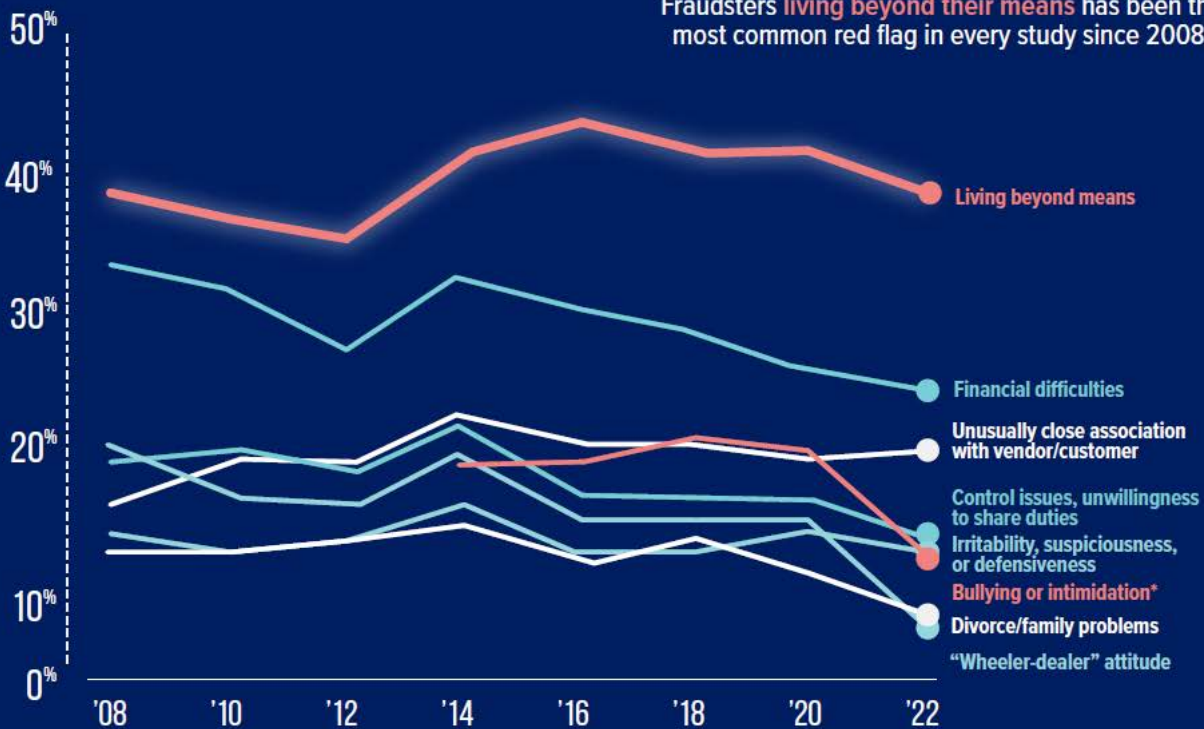
10%

"Wheeler-dealer" attitude

LIVING BEYOND MEANS



Fraudsters **living beyond their means** has been the most common red flag in every study since 2008.



* "Bullying or intimidation" was included as an option in our survey beginning in 2014 and was asked in a separate question prior to 2022.



The fraud risks posed by Artificial Intelligence

Alun Gordon, Local Counter-Fraud Specialist



Artificial intelligence (AI) is the development of computer systems that can perform tasks that typically require human-like intelligence, such as learning, problem solving and decision making. AI technologies are used in a wide range of applications, including speech recognition, language translation and image recognition.

Alun Gordon, Local Counter-Fraud Specialist explained: "AI can be used for both legitimate and illegitimate purposes. There is the potential for AI to be used to facilitate fraudulent activities, such as generating fake or misleading information, or automating scams or other fraudulent schemes. AI can also be used to detect and prevent fraud by analysing data and identifying patterns that may indicate fraudulent activity."

The use of AI in fraud depends on how it is implemented and used. Individuals and organisations should be aware of the potential risks and take appropriate measures to protect themselves from fraudulent activity, whether it involves AI or other technologies."

Why would a criminal use AI for fraudulent purposes?

- **Speed and efficiency:** AI can process large amounts of data and perform tasks quickly, which makes it a potentially useful tool for automating fraudulent activities.
- **Anonymity:** AI can be used to carry out fraudulent activities without leaving a traceable human trail.
- **Evasion of detection:** AI can be used to generate fake or misleading information that is difficult for humans to detect as fraudulent.

- **Personal gain:** Fraud is often motivated by a desire to obtain financial or other benefits through deceptive or dishonest means. AI can be used as a tool to facilitate this type of activity.

- **Generating fake or misleading information:** AI can be used to create fake websites, social media accounts, or other online content that is designed to deceive or mislead people. This could include generating fake reviews or manipulating online ratings to mislead consumers.

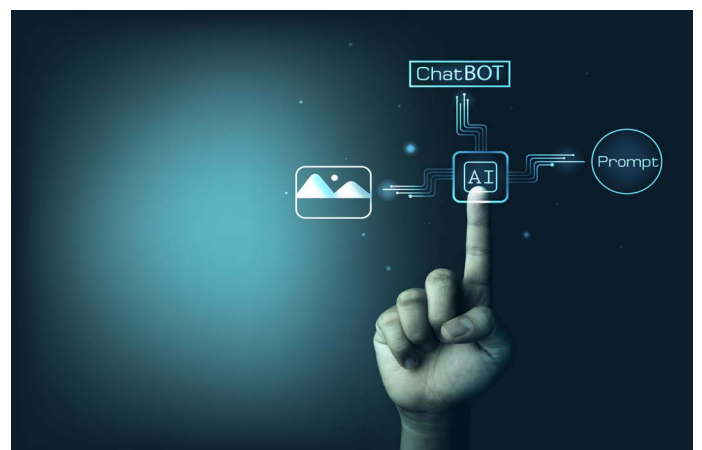
- **Automating scams:** AI can be used to automate scams or fraudulent schemes, such as by sending out mass emails or text messages that are designed to trick people into revealing sensitive information or sending money.

- **Spoofing phone numbers or email addresses:** AI can be used to create fake phone numbers or email addresses that are designed to deceive people into thinking they are communicating with a legitimate entity.

- **Generating fake documents:** AI can be used to create fake documents, such as contracts or invoices, that are designed to mislead or deceive people.

- **Evasion of detection:** AI can be used to evade detection by generating fake or misleading information that is difficult for humans to identify as fraudulent. This could make it more difficult for authorities to identify and track down cybercriminals.

- **Increased sophistication of attacks:** AI could be used to increase the sophistication of cyber-attacks, such as by generating more convincing phishing emails or by adapting to the defences of targeted organisations.





The fraud risks posed by Artificial Intelligence

How can NHS staff and NHS organisations avoid becoming victims of an AI-Assisted fraud?

- **Implement strong security measures**, such as using unique passwords for all accounts, enabling two-factor authentication, and keeping all software and security protocols up to date.
- **Educate yourself about the common signs of fraudulent activity**, such as unsolicited requests for personal information or offers that seem too good to be true.
- **Be cautious about sharing personal information.** Be selective about the personal information you share online and be cautious about responding to requests for personal information from unknown sources.
- **Report suspicious activity.** If you come across suspicious communications, report it to [Action Fraud](#)
- **Verify the authenticity of information and communications.** Be skeptical of information and communications that seem suspicious or too good to be true and take steps to verify their authenticity before acting on them.

Try Genie, Norton's new AI-powered scam detector that can determine if the text in an email is a phishing or text in SMS is smishing. Here: [Free Scam Detector - Prevent Phishing Scams - Genie by Norton](#)

WhatsApp Group Scam

It has become widely known that WhatsApp has been used by fraudsters to target individuals for nefarious purposes, including the recent "[Child's phone smashed](#)" scam. However, there is a new WhatsApp scam that targets large community and religious WhatsApp groups in operation (such as alumni and academic groups, work groups, and religious / prayer groups).

The fraudsters infiltrate the WhatsApp groups, and then target the members of these groups to try and deceive them into sending them money. Hundreds of people have fallen for this scam this year alone.

The fraud often starts when a group member receives a WhatsApp audio call from the fraudster, pretending, or claiming, to be another member of the group. The aim here is attempt to gain the targeted individual's trust, and beware, the fraudster may be using either a false profile picture/display name, or both, so at first glance it may appear to be a genuine member of the group that you know.

The fraudster then later calls the victim again (by this time they will be trusted by the targeted individual), informing them that they are sending a one-time passcode which will allow them to join an upcoming video call for group members. The scammer will ask the victim to share this passcode with them so they can be "registered" for the video call, but this isn't what is really taking place.

What will be happening is that the scammer has asked for a registration code to register the victim's WhatsApp account to a new device where they then take control of the victim's WhatsApp profile.

Once they have access to a victim's WhatsApp account, the fraudster will set up two-step verification which makes it impossible for the victim to then access their account. The scammer will then message other members of the group, or friends and family in the victim's contacts, asking them to transfer money urgently as they are in desperate need of help.

It is clear we all need to be wary when receiving contact via WhatsApp or other messaging platforms.

To avoid becoming a victim:


- Set up two-step verification to give an extra layer of protection to your account. Tap Settings > Account > Two-step verification > Enable.
- Never share your account's two-step authentication code (that's the six digit code you receive via SMS).
- If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- 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.



If you have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040.



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

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

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

Paul Bell
Senior Anti-Fraud Manager
 07552 253068
 Paul.Bell@miaa.nhs.uk



Phillip Leong
Anti-Fraud Specialist
 07721 237352
 Phillip.Leong@miaa.nhs.uk



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

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



Virginia Martin
Anti-Fraud Specialist
 07551 131109
 Virginia.Martin@miaa.nhs.uk

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

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

Karen McArdle
Anti-Fraud Specialist
 07774 332881
 Karen.McArdle@miaa.nhs.uk

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

Paul McGrath
Anti-Fraud Manager
 07584774761
 Paul.McGrath@miaa.nhs.uk