tiaa

FRAUD DIGEST

Edition 8
2024

THE CHANGING NHS FRAUD LANDSCAPE

Analysis of Trends

→ SEE PAGE 3

The Rise of Artificial Intelligence

→ SEE PAGE 4

Fraud Smart and Fraud Check

→ SEE PAGE 5

Introduction

In 2024, the fraud landscape within the National Health Service (NHS) continues to be a significant concern. The number of fraud investigations undertaken in the NHS for England and Wales increased by 56% from 2022/23 to 2023/24.

In response to the increasing volume and levels of sophistication in fraud offences, strategies to tackle fraud and error across the NHS have developed significantly in recent years and include:

1. Cross Government Counter Fraud Functional Strategy 2024-2027:

- The UK government is committed to tackling fraud across all sectors, including the NHS.
- The Counter Fraud Function collaborates with experts to efficiently combat fraud.
- Notable progress has been made, aided by technology and AI, making it harder for fraudsters to operate successfully.
- The Government Counter Fraud Profession (GCFP) supports professionalisation in counter fraud roles.

2. The NHS Business Services Authority (NHSBSA) Fraud, Error, and Loss Strategy 2024-2027:

- The NHSBSA emphasises flexibility to address the ever-changing fraud landscape.
- Collaboration with partners, and sharing best practice remains crucial to protect public funds.

3. NHS Counter Fraud Authority (NHSCFA):

- The NHSCFA play a critical role in improving departmental performance in tackling fraud.
- Projects have been developed to tackle fraud in the NHS that include:

Project Athena – A new way of fighting fraud in the NHS

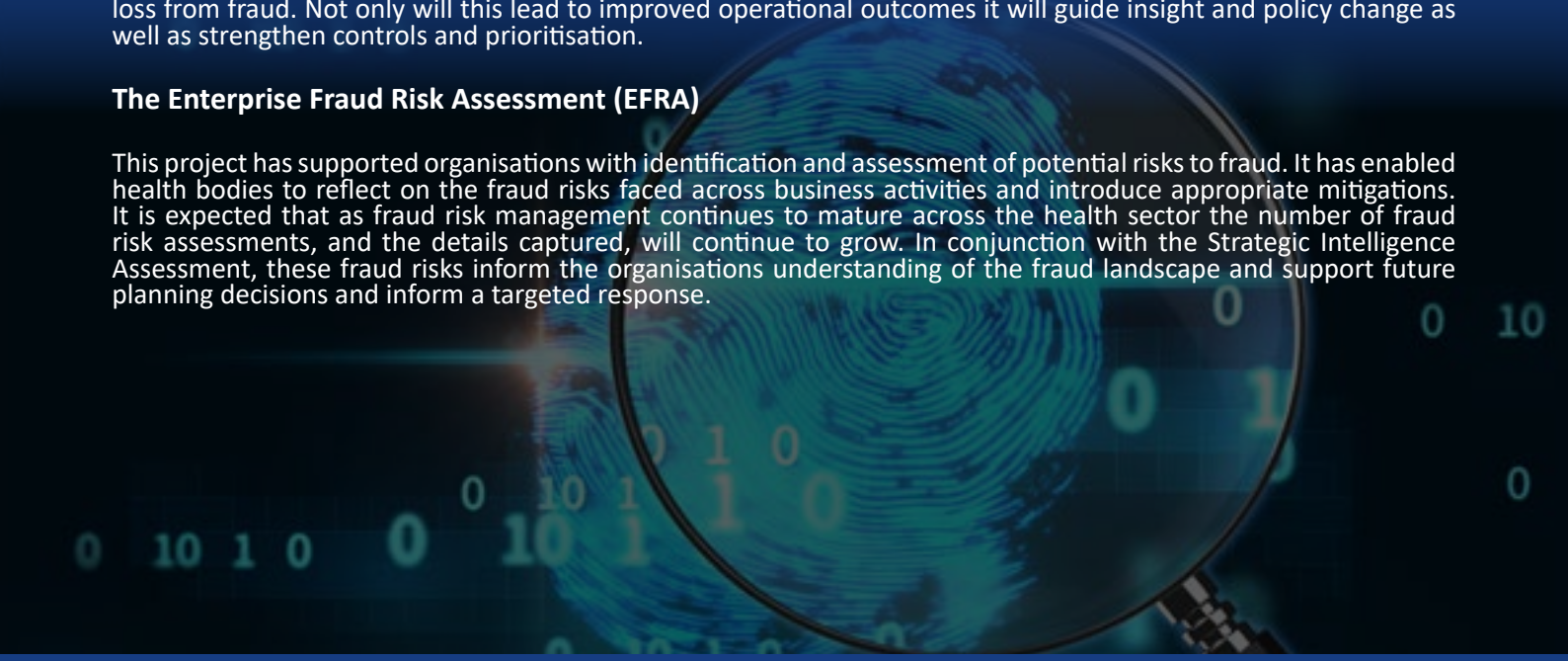
This is an innovative project to find fraud and prevent losses to the NHS through the way data is collected. It is a new pilot project aiming to prevent fraud and provide a dedicated response by identifying patterns in data on a scale that has never been done before across the NHS for counter fraud purposes.

It gives the NHSCFA the expertise to concentrate on significant areas using data analytics. This means that not only can more fraud be detected, but also prevented.

By anticipating and identifying new and emerging patterns in data, the NHSCFA can quickly reduce the effects and loss from fraud. Not only will this lead to improved operational outcomes it will guide insight and policy change as well as strengthen controls and prioritisation.

The Enterprise Fraud Risk Assessment (EFRA)

This project has supported organisations with identification and assessment of potential risks to fraud. It has enabled health bodies to reflect on the fraud risks faced across business activities and introduce appropriate mitigations. It is expected that as fraud risk management continues to mature across the health sector the number of fraud risk assessments, and the details captured, will continue to grow. In conjunction with the Strategic Intelligence Assessment, these fraud risks inform the organisations understanding of the fraud landscape and support future planning decisions and inform a targeted response.



Analysis of Fraud Trends Between 2022/23 and 2023/24

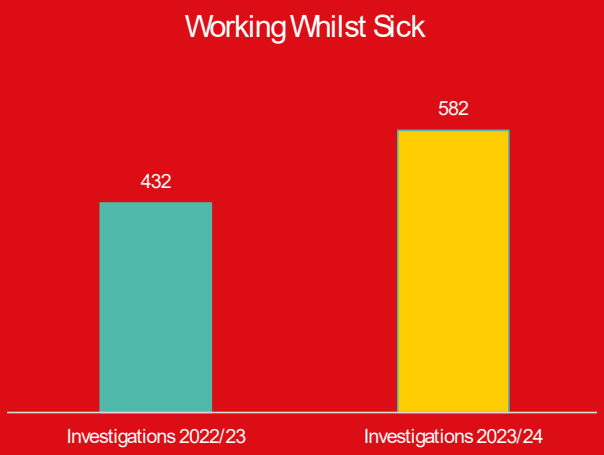
The overall number of NHS fraud investigations opened in England and Wales during 2023/24 increased by 56%, when compared against data for 2022/23. The rising cost of living has outpaced salaries, and this is likely to have contributed to an increased level of employee fraud.

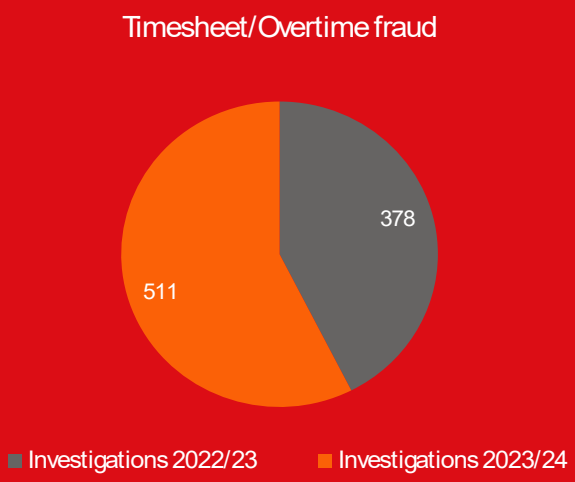
The Top 3 areas of employee fraud as shown in the graphs are:

Working Whilst Sick - This relates to someone working in the NHS who has falsely claimed they're sick when they are actually fit and undertaking work for another organisation.

Timesheet/Overtime - This relates to entries on a timesheet which are false or where the authorising signature has been falsified.

Recruitment Process / Employee Declaration - This relates to an employee providing false information or documentation to gain employment.





Emerging Fraud Trends

Emerging fraud trends facing our clients in 2024 include:

Mandate Fraud / Payment Diversion:

Activity across the NHS in preventing payment diversion fraud, also known as "mandate fraud", achieved savings of £4.8 million in 2023 to 2024. Payment diversion fraud is a criminal activity whereby health bodies are deceived into changing the payment details of those to whom they make payments for goods and services. The deceit sometimes involves the hacking of NHS staff email accounts and/or the use of almost identical email domains. If the fraud is successful, monies paid into the bogus accounts are swiftly withdrawn by the fraudsters and dispersed.

The Rise of Artificial Intelligence

The rise of artificial intelligence (AI) is significantly impacting the UK, particularly in the realm of cybercrime and fraud:

Concerns from Chief Internal Auditors:

Chief internal auditors express worry that cybercriminals will weaponise AI to commit more sophisticated and dangerous crimes. Nearly 78% of these auditors believe AI will negatively impact cyber security and data security, while 58% think it will exacerbate fraud (ICAEW Insights, 2024).

Deepfake Incidents Surge:

The UK has experienced a 300% rise in deepfake cases from 2022 to 2023, with a 780% increase across all of Europe (ITsec Bureau, 2023). Deepfakes are images, videos, or audio which are edited or generated using artificial intelligence tools, and which may depict real or non-existent people. Deepfake audio and video can deceive individuals into transferring large sums of money.

AI-Powered Cybersecurity Solutions:

Organisations are advised to deploy AI tools as part of their cyber defences. AI-powered cyber security solutions can detect ransomware in seconds. Staff should also be trained to recognise subtle signs of phishing emails, including email aliases and unusual URLs.

Human Element Remains Vital:

While AI plays a crucial role, we must not overlook the human element in cyber security. Staff confidence in challenging unexpected finance or data-related requests is essential to prevent fraud.

Overall, AI has both facilitated and complicated fraud. AI-driven fraud can however be combated, and consideration should be given to the following:

- **Synthetic Identities:**

  Fraudsters combine real and fake data to create convincing fake identities.

  Countermeasure: Employ multi-layered fraud prevention approaches, share knowledge through data exchanges, and enhance identity verification processes.

- **Phishing Scams at Scale:**

  AI assists fraudsters in creating more convincing phishing emails.

  Countermeasure: Educate users about phishing risks, use AI-powered email filters, and verify requests for sensitive information.

- **Voice Cloning for Scams:**

  Fraudsters clone voices to redirect bank funds.

  Countermeasure: Implement voice biometrics, monitor unusual transactions, and raise awareness about voice-based fraud.

- **Deepfake Videos:**

  AI-generated deepfakes deceive victims for scams.

  Countermeasure: Enhance video authentication methods and educate users about deepfake risks.

Remember, vigilance and adaptive strategies are essential to stay ahead of AI-driven fraud. In summary, AI's impact on cybercrime and fraud necessitates vigilance, training, and robust defences.

Fraud Smart and Fraud Check

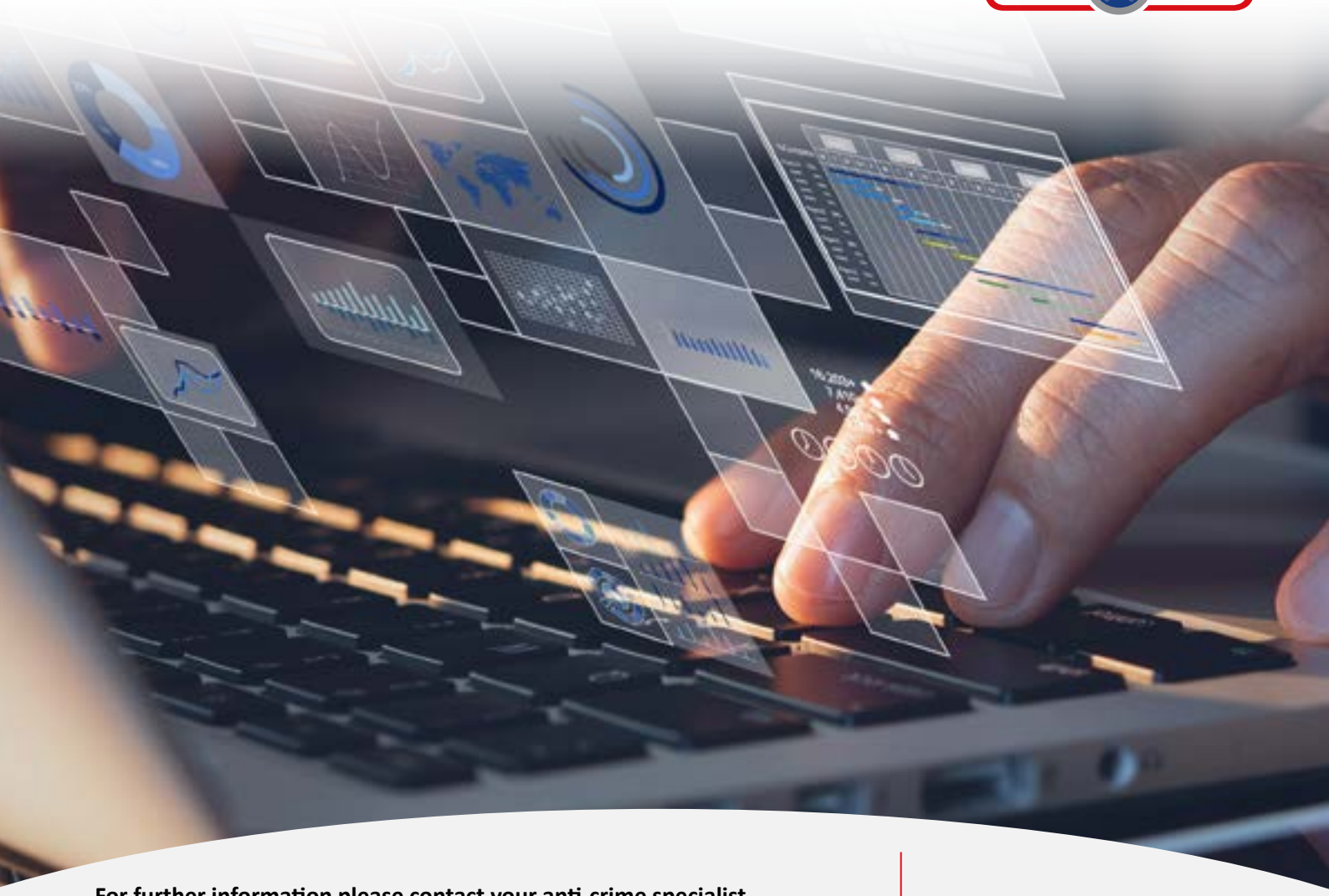
Any organisation can find themselves the victim of fraud and may have been scammed or involved in fraudulent activity at some time. New initiatives, such as “FraudSmart” and “FraudCheck” further support clients by identifying new and emerging fraud and economic crime trends which in turn assists organisations to develop strategies to combat fraud and to stay one step ahead in an ever fluid and challenging environment.

TIAA’s Fraud Intelligence Team proactively seek to identify such risks, issuing Fraud Alerts throughout the year. Often well in advance of those issued by the established regulatory body or industry associations.

Recent Fraud Alerts have been issued across all sectors and have included those concerned with phishing attempts, mandate and socially engineered CEO frauds, targeted attempts to steal salaries and the vulnerability of emails to tampering to name but a few.

Our Fraud Smart team are standing by to provide further support and advice. Our experts include investigators, forensic accountants, auditors and data management experts.

FRAUD SMART



For further information please contact your anti-crime specialist.

- **Melanie Alflatt,** Director - Risk and Advisory, melanie.alflatt@tiaa.co.uk
- **Andrew Ede,** Anti-Crime and Investigations Manager, andrew.ede@tiaa.co.uk