

THE CHANGING NHS FRAUD LANDSCAPE

**Analysis of
Trends**

→ SEE PAGE 3



**Post Covid
Fraud Risk**

→ SEE PAGE 4



**Fraud Smart
and Fraud
Check**

→ SEE PAGE 5



Introduction

In this Fraud Digest Update we review the projections outlined in our sixth annual digest against our half-year findings of the emerging internal fraud trends in the NHS.

In the sixth annual Digest we analysed new and emerging fraud trends and risks during the pandemic and sought to make longer term projections to changes in the fraud landscape.

We projected that firstly, as the country recovered from the pandemic, the economy would provide a driver on individuals and businesses to rationalise fraud. Secondly, we projected that remote working would create an opportunity for employees to commit fraud.

This was demonstrated by the 26% increase in fraud investigations amongst TIAA clients reported for the 2020-2021 year (compared to the 2019-2020 year) and supported by the findings of the Treasury Committee, who reported a 32% increase in fraud in the year ended June 2021, and reports in the national press.

For example, the Daily Mail recently reported that fraud has increased by up to 25% in the year to March 2022 with the proportion of those frauds being classed as cyber enabled fraud increasing by 8% up to 61%.

The Digest also projected a fall in fraud investigations for the 2021-2022 year. However, fraud trends evident towards the end of the 2021-2022 (that were not available at the time the Digest was published) began to suggest that fraud investigations were starting to increase again.

It was projected that there would be a secondary peak in fraud investigations for the 2022-2023 before fraud levels largely returned to pre-pandemic levels.

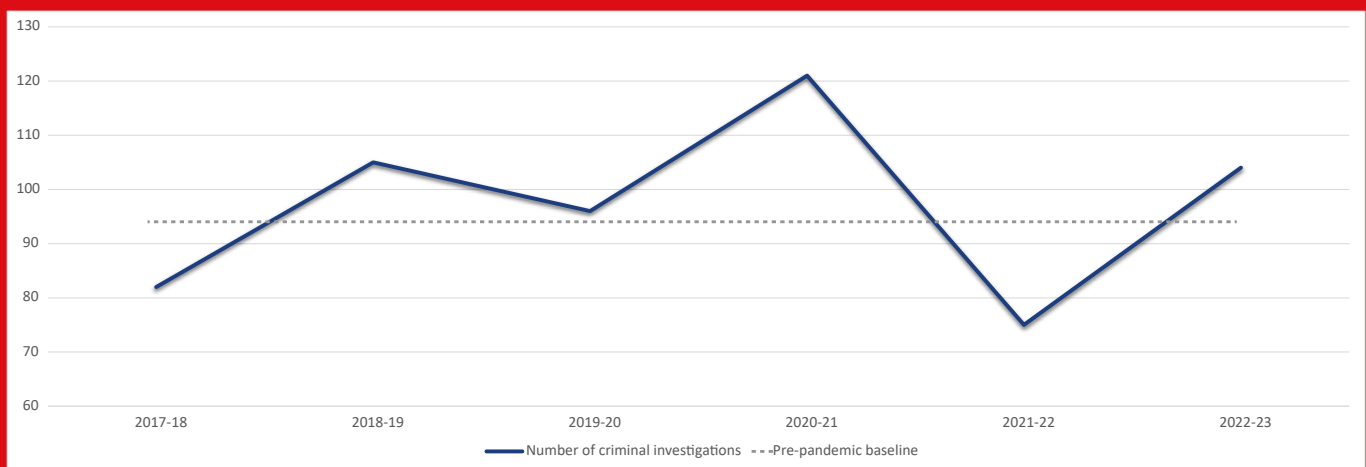
This update tests our projections against the first six months of data for the 2022-2023 year to establish whether the trends predicted have been realised.



Analysis of Fraud Trends

For the three years leading into the pandemic fraud levels averaged 94 criminal investigations. Analysis of fraud trends since the onset of the pandemic shows an immediate spike in reported fraud levels. This was particularly prevalent in the first two quarters of the 2020-2021 year and resulted in an overall increase of reported fraud for the year of 26%. Evidence shows this was caused primarily by increases in working whilst sick (WWS) (71% increase) and timesheet fraud (26% increase). It is of note that 30% of WWS frauds for 2020-2021 were linked to opportunities created by Covid-19. Wider environmental factors may have contributed to this trend such as heightened awareness of the NHS among both staff and the public resulting in increased reporting.

In the latter two quarters of 2020-2021 it became evident that reported frauds were slowing and this trend continued into 2021-2022. The sixth Fraud Digest projected criminal investigations for 2021-2022 of 52 whereas the final figure for criminal investigations was 75. The variance between projected and actual fraud levels can be explained by a spike in referrals received towards the end of 2021-2022 which continued into the first two quarters of 2022-2023.



The Current Risk Profile

- Analysis of the data reveals a growth in three fraud types is behind this, timesheet fraud, false vaccination records and mandate frauds.
- Timesheet fraud levels, year to date, stand at 21, compared with 15 for the whole 2021-2022 year. By year end they are projected to number as many as 44, constituting an increase of 193% on the previous year. When analysing the last 12-month period, 40% (14 of 35) of timesheets relate to duplicate employments which exploit remote working practices born from Covid-19 or exploit Covid-19 in other ways. This type of fraud has been identified as a risk across employers including the Ministry of Justice and Local Authorities.
- False vaccinations frauds were a new risk introduced by Covid-19 travel restrictions. Towards the end of 2021-2022 there were 11 incidents of false vaccination fraud with a further incident in 2022-2023. New incidents of this fraud type may dissipate but there is potential for historic frauds to be identified.
- Intelligence available to TIAA has shown a growing risk of cyber enabled fraud, particularly mandate frauds, for this year across sectors. Year to date there have already been three times the number of incidents than the previous two years. Whilst most of these have been unsuccessful TIAA are aware of one NHS body that has recently paid out £100,000s as part of a fraud.

Post Covid fraud risk- the outlook

National statistics show increasing fraud levels across all sectors during the pandemic years. Data specific to NHS bodies shows a large initial spike in reported fraud for the first year of the pandemic followed by a decline in reported fraud and then a secondary spike, beginning in the final quarter of 2021-2022 and continuing into this year. Current projections are for reported frauds to return to pre-pandemic levels by year end.

The pandemic has undoubtedly changed the fraud risk profile faced by the NHS with a number of emerging threats born from the changes to working practices that were brought about by this.

There has been a notable increase in timesheet fraud cases that exploit Covid-19, most notably overlapping or duplicate employments which exploit new remote working practices. The risk to employers is tangible and it is important that all policies and procedures relating to remote working and secondary employment are robust. Policies should be accessible, widely publicised and applied to both substantive and agency staff.

Organisations must have in place effective arrangements to manage staff working remotely.

Intelligence gleaned from across all sectors is showing

an increase in cyber enabled mandate type frauds. Due to the level of risk, it is vital that NHS bodies have a clear procedure on managing reported changes to suppliers' bank accounts and that key staff are fully appraised of this.

In addition, there are also a number of pandemic born risks that, whilst diminishing, have the potential for retrospective detection. Examples include false Covid vaccinations and false reporting of Covid sickness.

Finally, procurement fraud is an ongoing risk with reported losses amounting to £336million per year (Daily Mail September 2022). During the pandemic there were additional pressures on NHS bodies to modernise their estate and subsequent relaxation of procurement rules.

Therefore, the risk remains that frauds perpetrated during that time could subsequently be detected.



What should you do?

Increasing resource is vital. At a time where the economy is placing real challenges on household's income, fraud instances continue to evolve in complexity, volume and reach.

The typical approach is to cut back on back-office functions to make savings. In the past this included reducing investment in areas such as audit and anti-crime and is the opposite of what you should be doing.

A robust anti-crime solution is important. Targeting the areas below will ensure that you use your available resource effectively to obtain assurance of your organisation's fraud risk resilience.

- ✓ Evaluation of risk and intelligence
- ✓ A devised strategy
- ✓ Measurable outputs

Questions for the Audit Committee

- Are your remote working procedures robust?
- Are you managing the risk presented by remote agency staff in the same way as substantive staff?
- Are rules around disclosing secondary employment clear and applied to substantive and agency staff?
- Are your processes for dealing with supplier change of bank details clearly communicated to key staff?

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.



For further information please contact your anti-crime specialist.

- **Melanie Alflatt**, Director - Risk and Advisory, melanie.alflatt@tiaa.co.uk
- **Stuart Doyle**, Investigations Manager, stuart.doyle@tiaa.co.uk

The content of this document is intended to give general information only. Its contents should not, therefore, be regarded as constituting specific advice, and should not be relied on as such. No specific action should be taken without seeking appropriate professional advice.

