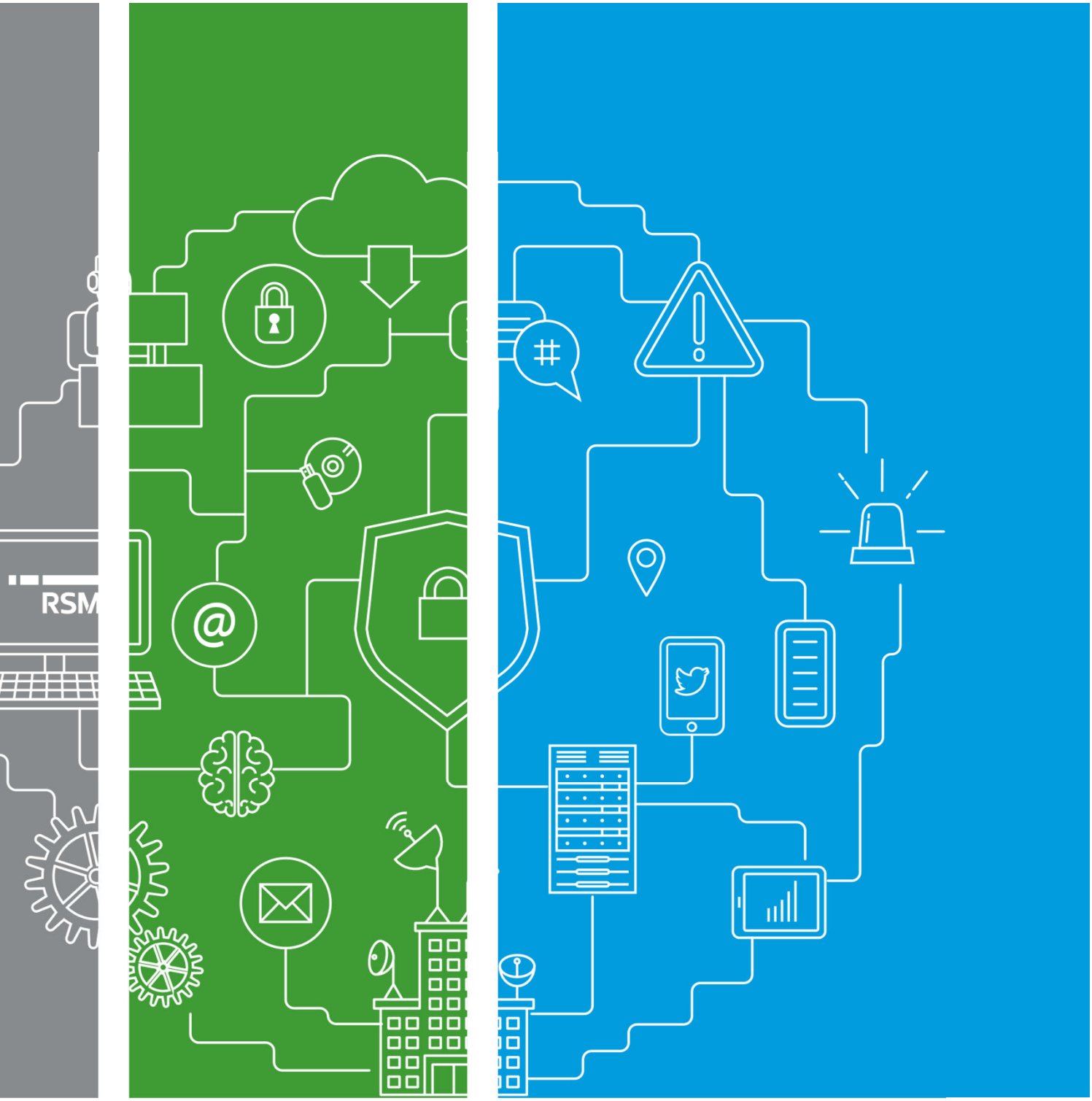


NOTICE FRAUD

For NHS organisations

Spring 2022

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

NOTICE FRAUD

Welcome to the latest edition of our counter fraud newsletter. In this issue we focus on current fraud trends across the NHS, providing you with insights into current fraud risk areas and details of some recent fraud investigations.

Alert – Vaccine Passport fraud/Misuse of Pinnacle

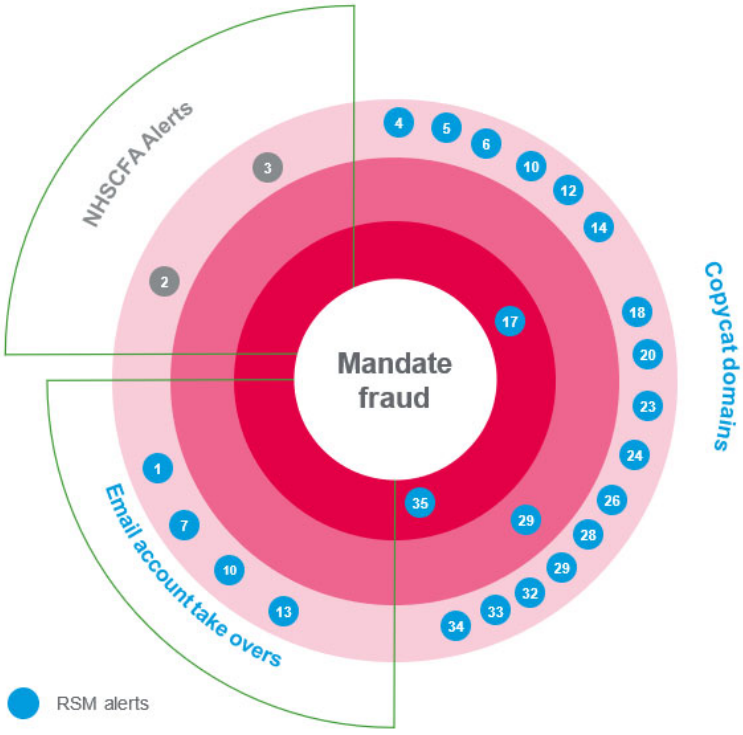
We recently shared a report of intelligence which suggested that some people are falsifying vaccine records in exchange for money. This action results in a patient showing as vaccinated on NHS spine when they have not received any vaccine which provides them with an official vaccine passport. This alert followed a news article that an individual in Hampshire had been arrested after being caught in a newspaper sting amending records for £750. Organisations should ensure that access to systems that can update vaccine records is only provided to those that need it, for the period they need it. You should also seek to review usage to identify any suspicious entries.

Alert – Data theft risk via DPA Subject Access Requests

An NHS body had been targeted by fraudsters who sought a staff member's personal and sensitive information through an intermediary company. The request specifically stated that identification should only be verified through the platform, and that no direct contact should be made which raised suspicions. On checking with the named member of staff, it was confirmed that they had no knowledge of the request or attempt to harvest details of them. Any SAR requests for employee information that are made indirectly should be verified with the member of staff directly and additional identification checks should be requested to verify the information is being sought by the employee.

Mandate Fraud

This remains a hotspot for fraud attempts at the moment. Fraudsters are attempting various methods to divert payment for either genuine invoices or are creating false invoices for work. Since April 2021 we have shared 22 mandate fraud alerts across our client base, representing a fraud prevention of £6,433,118.78, and all copycat domains have been blocked by NHS Digital and IT teams across the NHS. Please ensure appropriate processes are followed in all instances and if you have any reason for suspicion, please report your concerns and validate all details prior to sending any payments.



Financial Loss
Other adverse impact
Preventative saving

Preventative savings (client base)
£6,433,118.78

RECENT FRAUD CASES

Nurse dismissed and in receipt of a criminal sanction for undertaking work whist on paid sickness absence from their substantive role.

Between April 2020 and February 2021, a Trust registered Nurse had taken three episodes of sickness leave, spanning eight months, during which time they were alleged to have undertaken work for a Nursing Agency.

Initial enquires corroborated the allegation and further investigation confirmed that the subject had in fact worked for the Nursing Agency on 130 separate occasions, during which time they should have been working for the Trust. This resulted in a loss to the Trust of £6,940.23 in sick pay.

Following a parallel HR disciplinary investigation, the subject was dismissed from the Trust as a result of a hearing. They will also receive a conditional police caution, and have agreed to repay the funds to the Trust.

Organisations should seek to share such examples with staff to act as a deterrent to others, and encourage staff to share similar examples they identify.

WorldPay card terminals targeted by fraudsters.

A Trust suffered loss of £230k as a result of card payment terminal fraud. There were several hand held payment terminals used by the Trust, mainly by the cash offices, catering departments and pharmacies across all sites. These terminals are hosted by WorldPay, to whom the Trust pay a daily charge for the processing of transactions on the Trust's behalf.

Through reviewing recent statements for WorldPay, the Trust noticed 45 individual refunds to the sum of £230,100. Enquiries with WorldPay confirmed refunds had been sent to 21 separate bank accounts.

It was established that refunds are only possible with a supervisor passcode. However, in this case, the supervisor code had not been changed from it's original default code.

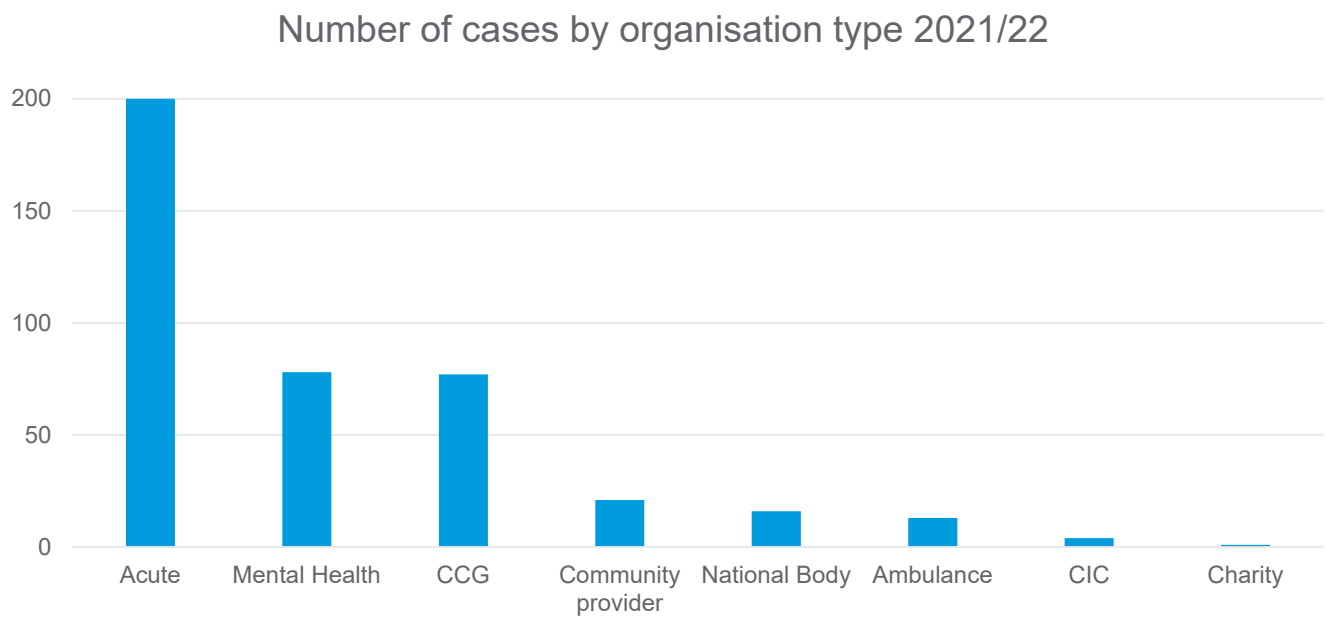
On reviewing CCTV evidence provided by the Trust, three young males were seen to enter the Trust in the early hours on three separate dates and reach under the glass to access the terminal.

The three suspects returned to the Trust on a fourth evening and were recognised by the Security team, who quickly contacted the police and detained them until their arrest.

An alert was shared with all RSM's Health Sector clients, and subsequently by the NHS CFA advising:

- Organisations should ascertain how many point of sale terminals are in operation, and ensure these are securely stored away from public access when not in use.
- All terminals should be updated to change the supervisor password from the default one provided.
- Guidance should be disseminated to all points of sale, security and security management to make them aware of this risk.
- Any out of hours visitors should be appropriately vetted before being granted access to the premises.

CURRENT REFERRAL TRENDS ACROSS RSM'S NHS CLIENT BASE



Throughout the period of 2021/22, we received a total of 543 referrals across our NHS client base. Of these, 410 resulted in investigations being undertaken.

For some context the NHS Counter Fraud Authority received around 2,000 information reports last year from 481 providers and commissioners, as well as NHS E&I, Resolution etc. The number of referrals we received across our from 61 NHS clients, accounted for around 25 per cent of all reported NHS fraud referrals.

Working whilst sick remains the area we have received most referrals in relation to. The following are the top six fraud areas reported to us during 2021/22.

- Working whilst sick
- Private work in NHS time
- Payroll/timesheets
- Invoicing mandate
- Misuse/theft of NHS resource
- Pharmaceutical patient

BEING ‘SCAM SAVVY’ IN THE CYBER WORLD

Cyber crime is a serious threat to organisations. With many of us working online, to protect yourself and your organisation, it is more important than ever that you, as the first line of defence, are aware of scams.

Back in 2017, over a third of England’s NHS Trusts were disrupted by the global ransomware attack known as ‘WannaCry.’ This ‘worm’ exploited a vulnerability within the Windows operating systems and locked up the files, which could only be accessed through payment of a ransom in bitcoin. No NHS organisation paid the ransom but it is estimated that disruption to services cost the NHS around £92m. This could have been largely avoided, had many of the NHS victims kept their systems up-to-date with security patches and this highlighted the importance of basic security practices.

Cyber criminals are firmly focused on the UK market. The past 12 months have seen the threat amplified by the coronavirus pandemic, as cyber criminals try to capitalise on the chaos. Our Cyber Security 2021 survey found that 20 per cent of organisations had experienced a cyber attack in the last 12 months, and 71 per cent of respondents said the attack was a direct result of the coronavirus pandemic.

95 per cent of cyber security breaches are due to human error, so user behaviour and education is the best way to protect your organisation against many of the most common scams.

Areas where cyber scams are common:

- Invoice mandate fraud
- Salary payment diversion fraud
- Email interception
- Targeted phishing emails and fraudulent links
- Malware

CONTACTS

RSM Counter Fraud Team:
Matt Wilson
Associate Director (LCFS)
matt.wilson@rsmuk.com

Kirsty Clarke
Senior Consultant (Lead LCFS)
kirsty.clarke@rsmuk.com

Counter Fraud Champion:
Andrew Spicer
andrew.spicer1@nhs.net

Chief Finance Officer:
Simon Goodwin
simon.goodwin1@nhs.net

RSM UK Risk Assurance Services LLP
25 Farringdon Street
London
EC4A 4AB
United Kingdom
T +44 (0)20 3201 8000
rsmuk.com