



FRAUD IN THE NHS, A YEAR ON

Benchmarking fraud 2015

EXECUTIVE SUMMARY

Benchmarking reactive fraud referrals across the NHS.

RSM works extensively across the NHS and delivers counter fraud services to over 80 clients nationally as the local counter fraud service (LCFS).

We outline a number of fraud related issues captured through our case management system. It has been a year since we last published our outcomes. Our new findings and comparisons against last year's findings remain interesting to see where fraud has increased or remained static, as well as the emergence of new types of fraud risk.

Based on our figures, fraud in the NHS has increased by 17 per cent since last year. Does this mean there is an increase in fraud or has there been an uplift in the number of reported instances of fraud? The increased focus on whistleblowing and raising concerns has had a positive impact on the willingness and ability to identify and report concerns.

Providing assurance and directing resource in areas that require greater focus should be high on the agenda. Certainly fraud is an area to take seriously and reflect upon in the coming financial year as many audit committees are looking for comparative data to help them assess their counter fraud arrangements and fraud risks.

16%

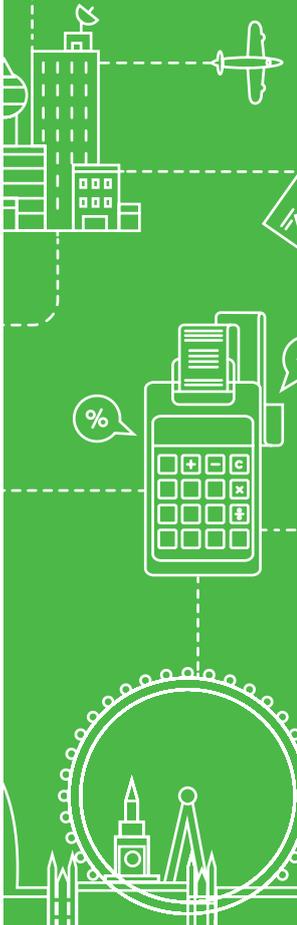
of NHS fraud referrals relate to employees undertaking unauthorised work whilst on sick leave.

9%

of NHS fraud referrals relate to the theft/misuse of NHS resource and to staff altering/falsifying timesheets.

CONTENTS

| | |
|---|----|
| Executive summary | 3 |
| Overview | 5 |
| What is the real picture? | 6 |
| When are referrals most likely to take place? | 7 |
| Where do referrals come from? | 8 |
| Who is committing fraud? | 9 |
| Recoveries and sanctions | 12 |
| Emerging risks | 13 |
| Case studies | 14 |
| Contact us | 16 |



OVERVIEW

The total value of fraud is likely to be much more significant than £12m, but much still remains unreported or undetected.

Due to the nature of fraud in general and the on-going changes and pressures being faced by the NHS, it is an important time to carefully consider your programme of proactive counter fraud in order to minimise the risk of occurrence.

Fraud costs any business, and the ability for the NHS to assign finances to the core function of providing first class patient care must be a primary focus. Difficult decisions regarding the use of resources take place daily. Losses to fraud will be reduced by a targeted risk based resource, underpinned by specialists to take on effective work in areas where risks are most prevalent.

Pressure is increasing year on year to deliver high quality services with reduced finance and resource, resulting in the need to adapt delivery approaches. Reducing the focus on governance, by using less people to do more, is in itself a short sighted approach to cost cutting. Using a modern risk based specialist counter fraud service as part of your governance toolkit, will lead to a positive impact on savings and a reduction in fraud instances and controllable risks. Doing nothing or the using the same methods should not be an option. the risks associated with not tackling fraud are more than losing money, it can lead to a negative impact on delivery of service, damage morale of staff and confidence from service users. In addition, damage to your reputation could prove irreversible

NHS Protect has reported that the total value of identified fraud in the NHS during 2014/15 was just under £12m.



WHAT IS THE REAL PICTURE?

A total of 364 reactive referrals were received this year. An increase from last year of 17 per cent.

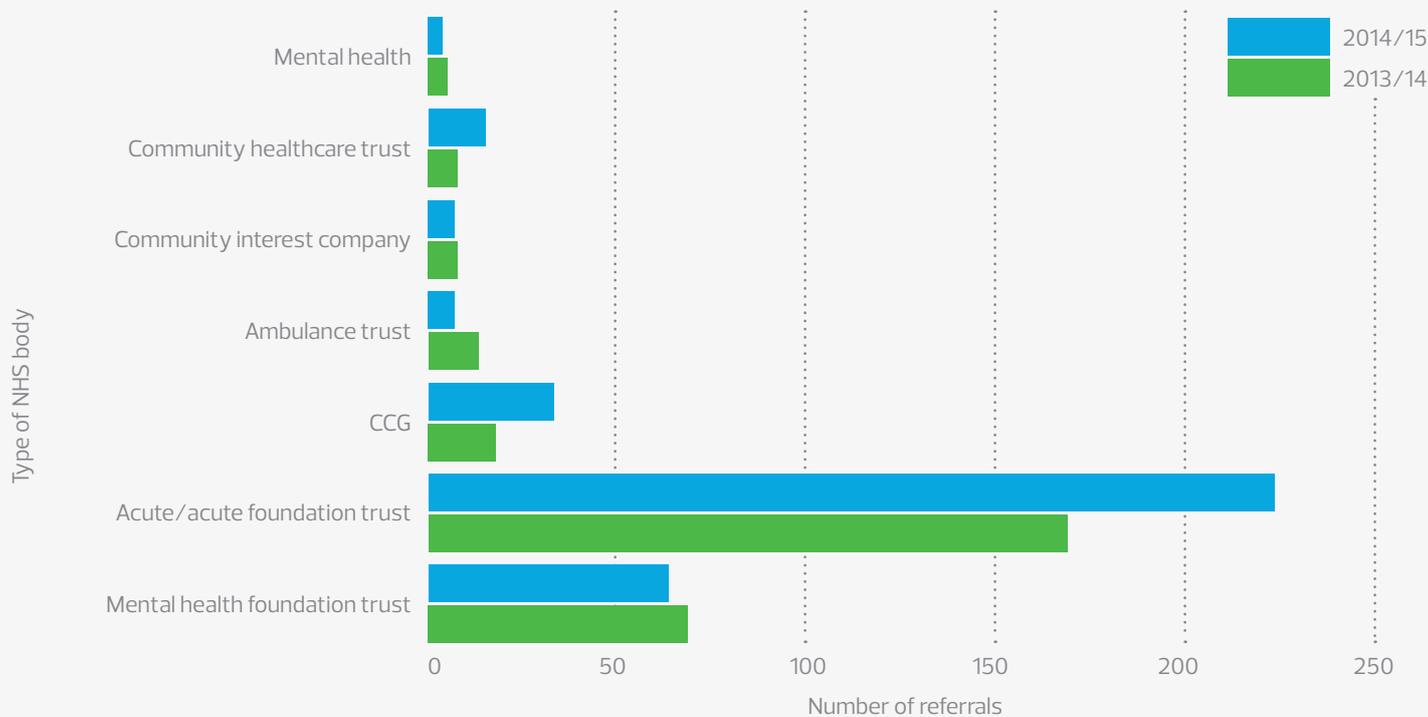
The question we often get asked is whether fraud is actually increasing or just being reported more. The answer to both, based on our experiences and industry views, is yes.

More fraud appears to be happening, however, we firmly believe that awareness and detection has also improved. With the level of publicity around instances of fraud, there is less tolerance of accepting it and reduced likelihood of ignoring it.

Fraud is not a victimless crime, a view shared by our clients and the wider public.

Of particular note, and demonstrating the development of the counter fraud provision amongst clinical commissioning groups (CCGs), we have seen an increase in the number of referrals to 83 in CCGs. This is a positive outcome of our focussed awareness programmes and fraud risk assessments.

We anticipate this trend to continue during the current financial year, as further proactive work is undertaken in key risk areas. Comparative data shows us that acute and acute foundation trusts remain the source of the highest overall number of referrals.

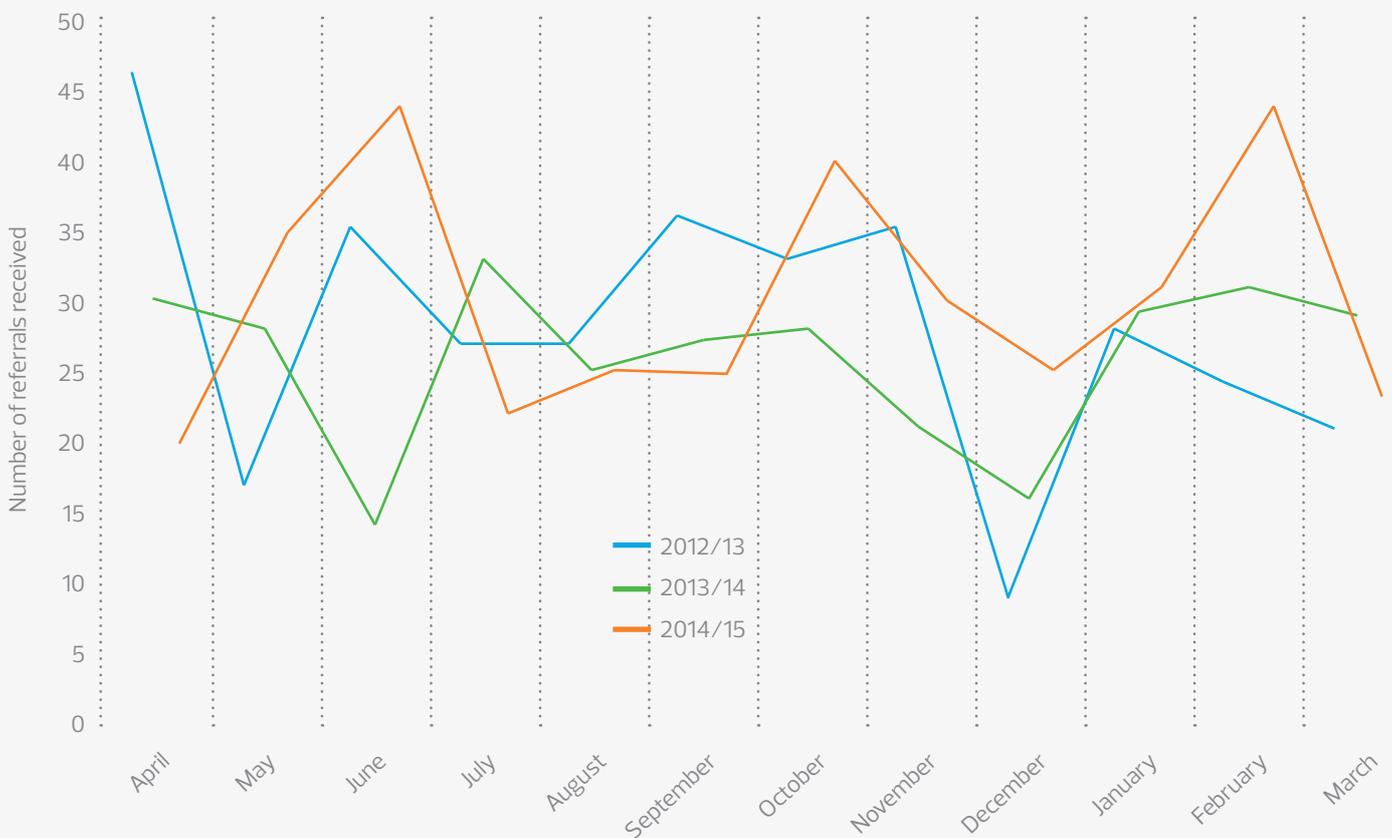


WHEN ARE REFERRALS MOST LIKELY TO TAKE PLACE?

The number of referrals received each month was on average 30, with a month on month peak in both June 2014 and February 2015.

As in previous years, we have noticed a steady increase in referrals made directly following 'fraud awareness month', our national awareness initiative which we encourage our counter fraud clients to support. This took place in January 2015.

It is possible that peaks in June and October occur due to seasonal holiday periods, whereby processes and fraudulent activities can become more visible, because roles may be covered during staff holiday by temporary staff or by staff on rotation of duties. It is all too common that frauds get uncovered when those committing them are away on periods of absence from the workplace, as they are not able to sufficiently cover their tracks. Also, staff may feel more comfortable reporting concerns when their colleagues are away.



WHERE DO REFERRALS COME FROM?

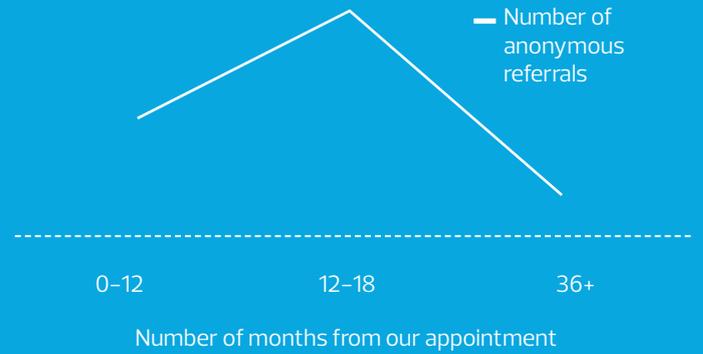
Understanding the source of referrals provides insight on how to shape future awareness activity.

Both last year and this year, the majority of referrals came from existing key contacts within NHS organisations, specifically the HR function who work alongside the LCFS in all investigations, as well as other key department managers.

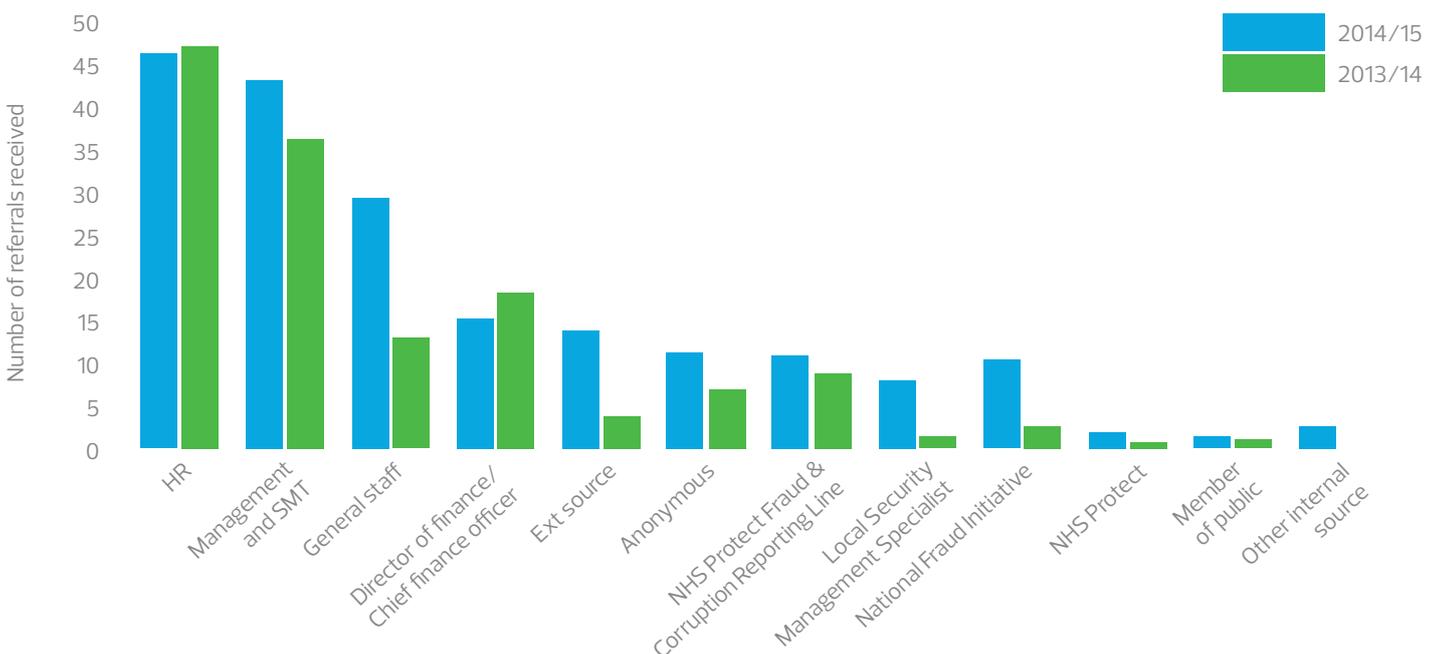
The level of anonymous referrals increased although the vast majority of referrals are made by named individuals. Referrals from general staff and external sources nearly doubled in the last year which shows a positive change in the culture and general acknowledgement of fraud across the NHS.

By operating on a visible and supportive basis we ensure our counter fraud approaches instil confidence and inclusivity. Initial spikes in referrals between 12 -18 months are likely as confidence in the policies improves. As represented here referrals, are seen to decline as counter fraud practices fully embed within an organisation.

NUMBER OF REFERRALS

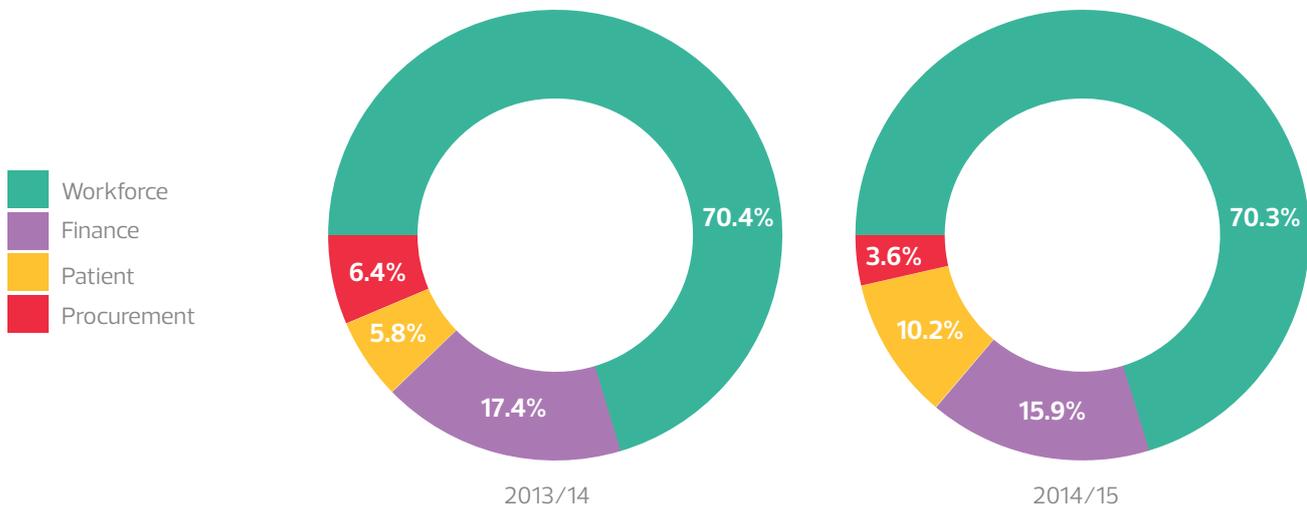


A good working relationship between the LCFS and key department heads is critical to the delivery of a successful counter fraud programme. Trends show that referrals should decrease over time, with quality and conversion of referrals to investigations should increase as awareness becomes embedded.



WHO IS COMMITTING FRAUD?

The referrals we received in 2014/15 fall in to four main categories:



Of the referrals we received, they predominantly occur within four distinct areas, workforce, finance, patient and procurement. It is interesting that three of the four areas fall directly within the operations of the NHS and fraud remained constant across finance and workforce fraud.

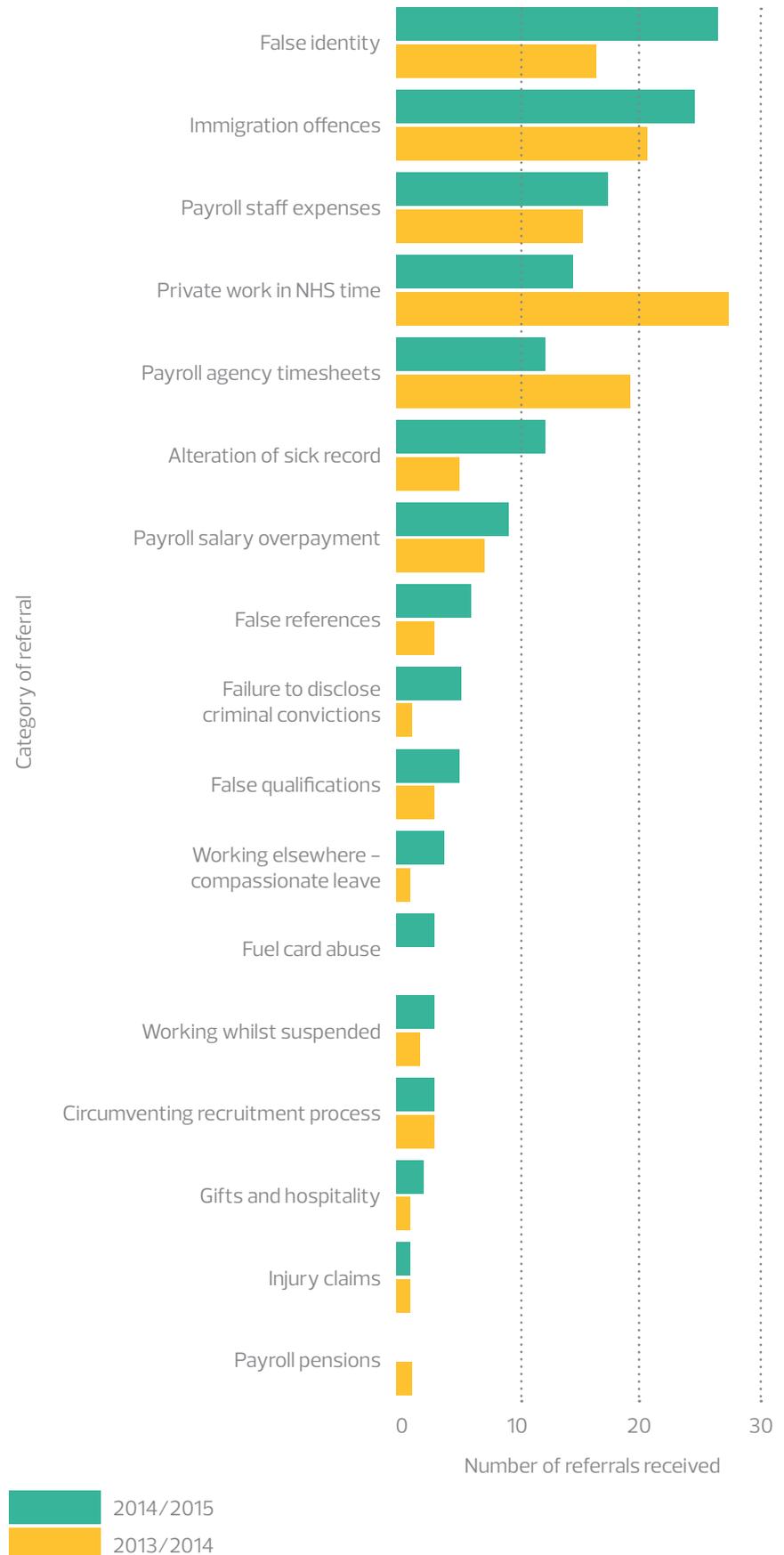
The reduction in procurement fraud is almost certainly attributed to the work we have done with clients during the last year to focus on compliance with the NHS standards for procurement. NHS Protect has provided guidance and support within this area which has resulted in positive engagement and proactive work. Additionally, the introduction of our fraud awareness month initiative and the increased on-site awareness this created amongst both staff and patients could have had an impact on the number of patient frauds having been referred.

The nature of referrals we have received are in line with those reported by NHS Protect which identified the following as the most widespread fraud risk areas during this year:

- misrepresentation of qualifications/skills or experience;
- timesheet fraud;
- working while off sick; and
- expenses claims fraud.



To drill deeper into what this means, the workforce referrals covered a number of areas.



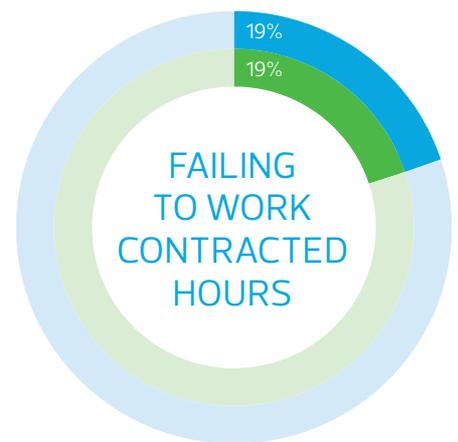
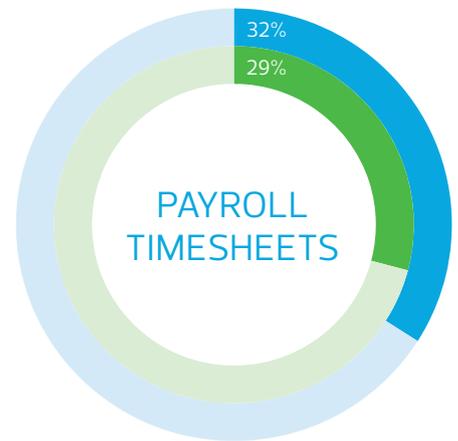
Over the last year, there was a considerable increase in allegations of identity fraud particularly within the recruitment process. Working whilst sick and falsifying payroll timesheets as well as staff failing to work their contracted hours remains largely constant from last year.

Most fraud is detected by staff. Therefore, delivering a robust and targeted programme of awareness and providing staff with the knowledge and confidence to spot and report concerns is vital, as well as advising staff on their responsibilities and increasing accountability to report fraud. Encouraging staff to take ownership of where they work and NHS resources will lead to further positive changes in culture.

We have found that implementing clear reporting lines, so that staff and users can report their concerns confidentially and appropriate action can be taken helps accountability. This approach also acts as a deterrent to the minority who choose to defraud the health service; because a function exists which will detect and take robust action in applying sanctions, including seeking redress, should they commit fraud.

Mandate and bank account fraud has decreased as a direct result of greater and proactive awareness, as well as detection work being done within finance departments. It is necessary to remain vigilant to the varying methods used by fraudsters.

Fraud involving identity crime and entitlement to work in the UK has increased since last year. We believe this to be following the trend where identity crime continues to rise across all sectors, with its detection to be improved due to the awareness, procedures and tools now in place across many of our clients.



RECOVERIES AND SANCTIONS

This year, over £688,000 of funds were secured for recovery or were prevented from being defrauded.

Additionally, our work resulted in seven criminal sanctions (of which two resulted in custodial prison sentences), five instances where civil recovery or repayment of funds were made, 24 disciplinary sanctions, including 12 resulting in dismissals and a further five cases where the staff being investigated resigned from their posts.

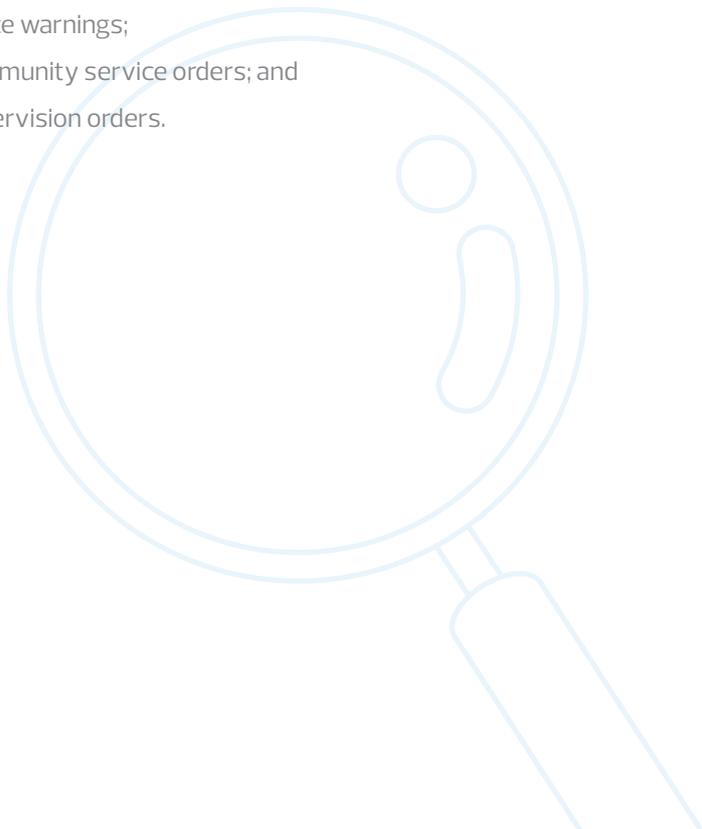
Upon concluding investigations, where appropriate, we work with our clients to recover monies as efficiently as possible. We do this either in line with criminal sanctions or via civil recovery. We will ensure that any instances of clinical or patient risk are well-thought-out and escalated to the client. The struggle lies in identifying the value of fraud deterred, by our clients and LCFS staff undertaking the proactive prevention work. However, the vast majority of staff and public are above board and honest, whereby simple controls and deterrence may be sufficient. Mobilising the honest majority through increased awareness and knowledge is a key tactic to improving overall governance. Thereby, targeted resources can be focussed on the minority who seek to defraud the NHS, regardless of the controls or measures in place to prevent such.

At the outset of every investigation, one of our priorities is to prevent on-going losses. Methods used to do this include:

- payroll deductions;
- NHS pension recoveries;
- confiscation orders upon successful prosecution;
- civil recovery proceedings using our relationships with specialist law firms; and
- repayment agreements.

The concluded criminal sanctions this financial year include:

- two custodial sentences;
- police warnings;
- community service orders; and
- supervision orders.



EMERGING RISKS

By providing counter fraud services extensively within the NHS, we are able to collate intelligence and data relating to fraud trends and emerging threats facing the sector. We horizon scan and make sure that we are truly proactive in alerting our clients to the emergence of fraud risks. This enables clients to take effective measures to prevent fraud from occurring from the outset.

The following outlines the key areas where we anticipate greater fraud risk in the coming year.

Employee internal fraud

A main area of risk, and should remain at the forefront. Most are opportunistic, however there are examples of organised employee fraud too:

- working elsewhere;
- false qualifications;
- private work in NHS time/use of NHS resources;
- immigration offences;
- gifts and hospitality;
- false identity;
- alteration of sick records;
- false references;
- payroll (timesheets; expenses etc); and
- failure to disclose criminal convictions.

Misuse/theft of NHS resources

There have been a number of cases where NHS employees have taken NHS resources. These include items being advertised for private sale on auction sites and also for use within/by private providers, at the cost of the taxpayer.

Recruitment fraud

Recruitment fraud occurs when false information is provided in order to gain employment. Examples include lying about employment history and qualifications and providing false identity documents such as untrue papers showing the right to work in the UK, as well as CV fraud. It is reported that the annual cost of this type of fraud in the UK is £616m. We expect this type of fraud to increase further.

Cyber enabled fraud

Recognised as one of the most significant areas of crime, the catalyst is not always fraud driven. However, cyber fraud is seen as a significant risk to businesses, with attacks on IT infrastructure increasing in frequency and sophistication.

This comes in various guises, but can have a significant effect, both financially by defrauding businesses of monies but also indirectly by way of 'distributed denial of service' type attacks and theft of data.

Intelligence from industry suggests that this type of fraud is emerging at pace. The National Fraud Intelligence Bureau outlines that over 70 per cent of reported frauds in the last year were computer or internet generated.

As a potentially destructive threat to organisations, the NHS and wider public sector need to consider the risks and review procedures in place inclusive of IT network security, how their IT infrastructure is used, data security and IT disaster recovery plans.

We have already experienced a significant increase in the variety, volume and sophistication of cyber attacks affecting the NHS in particular in:

- mass marketing frauds;
- 'phishing' or 'vishing' email type frauds; and
- e-commerce or online banking/transaction frauds.

Organised crime

Organised fraud knows no boundaries, whether by geographical location, sector or function. There have been several cases recently of organised crime groups targeting the NHS by defrauding finance departments of substantial sums through bank mandate fraud, or the placement of fraudsters into key areas for the sole purpose of defrauding NHS organisations. NHS Protect has successfully tackled several cases of this.

The most effective measure is to deploy an effective counter fraud provision, raising awareness among staff by empowering them to have the knowledge to spot the key fraud indicators (red flags) and clear confidential reporting lines to raise concerns. In addition, robust governance and a controlled environment is a vital line of defence in preventing your organisation falling victim.

CASE STUDIES

Some examples of where we have supported NHS clients deal with fraud.

Falsified timesheets result in custodial sentence, community service and order to repay almost £8,000 for an ambulance trust employee.

An employee was ordered to repay £7,838 and was sentenced to 16 months in custody, suspended for two years in addition to 200 hours community service after pleading guilty to one count of fraud by false representation.

The employee pleaded guilty after spending 13 months 'on the run'. In passing sentence the judge described them as 'someone who had abused his position within the NHS over a period of time and someone who was fully aware that he had no right to do so and as such acted in a dishonest and despicable manner and was someone who chose to attack the national treasure that is the NHS'.

The member of staff was employed as agency staff and was recruited into a full time post working as a Production Desk Assistant (call centre). Despite later being appointed as a full time member of staff, they submitted 16 false timesheets to the agency they had previously been contracted through. When questioned, they admitted that they had used the money to pay rent arrears and other debts they had accumulated.

Ambulance trust worker found guilty of fuel card abuse results in custodial sentence, unpaid work order and repayment of almost £4,000.

Another ambulance trust employee appeared before a magistrate court last April where they pleaded guilty to defrauding the trust of £3,758. The individual was sentenced to six weeks in custody, suspended for 12 months, 100 hours unpaid work, costs of £85, victim surcharge of £60 and ordered to repay the defrauded money.

The crime came to light after it was discovered that the employee had stolen an amount of diesel fuel through use of his fuel card. When questioned he failed to provide an explanation for his crime and instead he gave a 'no comment' interview.

National fraud initiative caught out illegal worker at acute trust, resulting in the recovery of just over £8,000.

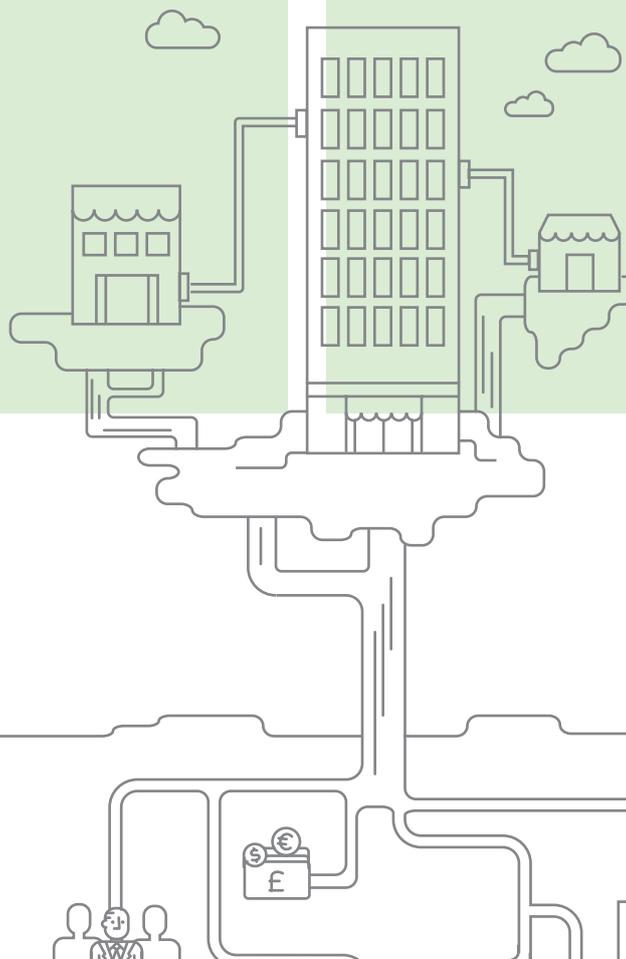
As part of one of our national fraud initiatives, an employee was highlighted as working without the correct rights to work in the UK. Following our enquiries and investigation, we found that they had produced falsified documents when they began working at the trust.

The case was heard at crown court and they were ordered to repay over £8,000 via deductions to their NHS pension contributions. As the individual was employed as a staff nurse, the matter was also referred to the Nursing and Midwifery Council. Needless to say, they were also dismissed from the trust in line with its disciplinary procedure.

A hospital patient falsely claimed travel costs, found guilty of fraud and sentenced to a six month community service and full repayment to the trust.

A staff member with a trust referred a suspected fraud to the LCFS for investigation. As a result, investigation identified an over claim by the patient.

It transpired that a patient submitted claims for travel to attend appointments which didn't exist. Whilst the claims resulted in a total amount claimed fraudulently of £146, the case was heard at a magistrates court and the patient sentenced to six month community service and a compensation order for the full amount to be paid back.



CONTACT US

As one of the leading external counter fraud providers in the UK, we have detailed knowledge of fraud and bribery matters within the NHS.

For information on how we can support you, please contact David Foley or your usual RSM counter fraud contact.



David Foley
Director of Fraud Risk Services

T +44 (0)20 32018000
david.foley@rsmuk.com

Our extensive team includes:

- Forensic accountants.
- Forensic investigators.
- Corporate financiers and due diligence specialists.
- Insolvency specialist investigations.
- Asset tracing and recovery services.
- Business Intelligence analysts.
- Internal auditors
- External auditors
- Contract risk specialists
- IT auditors.
- Forensic computer e-discovery specialists.
- Data analysts.
- Cyber-crime specialists.

Related links:

rsmuk.com/healthcare

rsmuk.com/fraudriskservices

rsmuk.com/technologyrisksolutions

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 11 Old Jewry, London EC2R 8DU. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Consulting LLP, RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.