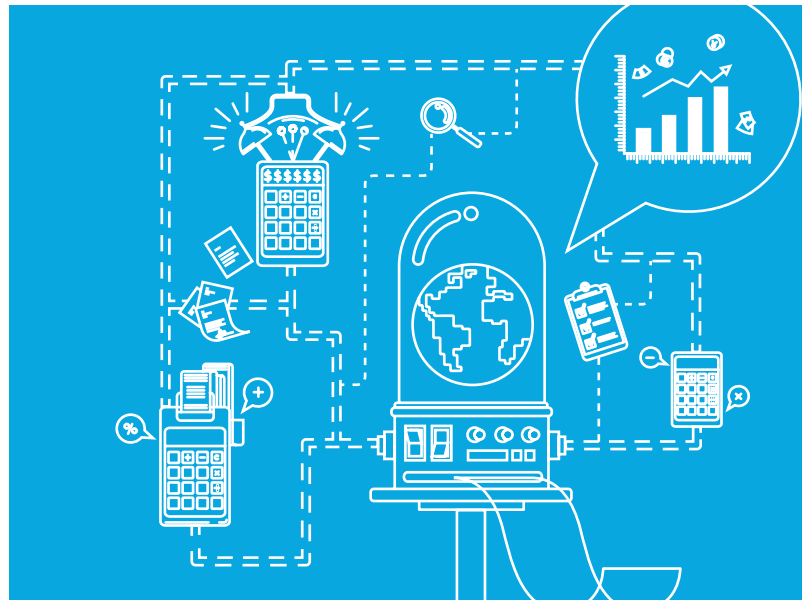


Notice Fraud

June 2018



This edition of Notice Fraud is designed to bring recent cases, emerging risks and scams to your attention to help you recognise the signs of fraud in the NHS.

Invoice fraud

Invoice fraud is closely linked to procurement fraud, as it includes any fraud in which steps were deliberately taken by the supplier to mislead a health body, with a view to obtaining payments that were not properly due. There are several types of invoice-related fraud, most commonly: suppliers submitting multiple invoices for the same work; suppliers over-billing for work; or employees creating 'dummy firms.'

Invoice fraud also includes 'change of bank account scams.' This occurs when a request is made by someone purporting to be from a supplier to the organisation. The request usually involves changing the details of a direct debit, standing order or bank transfer mandate.

Invoice fraud is not new and remains relatively simple. Prevention is key. The first line of defence for any organisation is their staff. Those with responsibility for paying or authorising invoices need to be aware of risks and the indicators of invoice fraud.

Preventing and detecting invoice fraud

- Staff are the first line of defence. Staff with responsibility for paying or authorising invoices, or for supervising these processes, should be aware of the risk of invoicing fraud.
- Check the details on the invoice eg invoice date, logos, supplier details or misspellings. If it is a regular supplier, check the information against the details you already hold.
- Match purchase orders / booking confirmations against invoices. Do they match with what was agreed? Are there any hidden charges?
- Check for changes in regular invoices. For example, the amount or the number of invoices received.
- Check for duplicates.

Locksmith used his position to defraud an NHS trust out of £600K

A locksmith at an NHS trust who was responsible for purchasing locksmith materials failed to declare he owned the company supplying the materials. He supplied the trust for six years and marked up some prices by up to 1,200 per cent.

The locksmith was jailed for six years. The NHS Counter Fraud Authority is pursuing recovery of the money defrauded.

'Inspirational leader of the year' defrauds the NHS

NHS England's former national lead for equality and former chief executive of an NHS trust authorised a £11,072 payment to her husband's graphic design business to produce a newsletter and a document about leadership for NHS chief executive officers.

The investigation identified that the leadership document was a scam containing other people's work cut and pasted from the internet, included empty pages, and was only produced after the investigation had commenced.

The former chief executive was stripped of her CBE in December 2017. She was given a 16-month prison sentence, suspended for two years and must do 250 hours of unpaid work. Her husband was jailed for 10 months, suspended for two years, and ordered to do 150 hours of unpaid work.

Both must repay £11,072 under the Proceeds of Crime Act.

New NHS England counter fraud team

NHS England has a new dedicated in-house Counter Fraud Team. The central team is based in Leeds and there are four regional teams located at NHS England local offices across the country.

The primary purpose of the team is to respond to and investigate allegations of fraud; the majority of NHS England fraud investigations relate to primary care.

If you have a specific concern of fraud and not sure whether it should be referred to NHS England, please speak to your own counter fraud specialist in the first instance.

Switchboard calls

We have become aware of a scam where calls are made to the switchboard claiming to be from staff members. The caller asks to be transferred to an external number which starts with 090 and incurs a significant charge per minute.

Organisations are advised to update their switchboard staff that calls must not be transferred to external numbers, and ensure that 090 calls are restricted on the network.

Current email scams

Email scams, also called phishing scams, are becoming increasingly common as fraudsters come up with new ways to try and trick you into clicking on a link or stealing personal information. We have listed below the current scams that you should be aware of.

Remember, if you are in any doubt about the origin of an email, do not open it.

Extortion phishing

Extortion phishing is the term used for obtaining something, usually money, through force or threats via email.

A client reported receiving several emails over a weekend. The emails suggest that the recipient has been recorded through their webcam whilst watching adult websites. The sender threatens to circulate the recording to the recipients' friends if a payment is not made within a set timeframe. The payment is requested in bitcoin.

As the email was sent through various sources the client was unable to create a simple block of the sender. Instead, they had to use a key word filter to generate a block.

NHS.net

Several NHS.net users have reported receiving an email with the subject 'suspicious url: urgent.' The email suggests that it is an NHS email update programme and the user must click on the link to update their email account. Do not click on the link and delete the email.

Emails are being sent to NHS.net accounts purporting to be from the DVLA. The email suggests that the recipient is eligible for a vehicle tax refund due to an overpayment. The DVLA said in a message on Twitter: 'We are aware of an email/text scam that asks drivers to verify their driving license and vehicle tax details via an online link... As it isn't from DVLA, please delete it and don't enter any of your details.'

Reporting concerns

If you have suspicions that fraud may be occurring or wish to receive further information about any of the above, please contact your Local Counter Fraud Specialist (LCFS).

Alternatively, you can report any concerns to the NHSCFA on 0800 028 40 60 (between 8am and 5pm, Monday to Friday) or via the online reporting form: www.cfa.nhs.uk/reportfraud. All information provided via this secure website is completely confidential.

It is the LCFS' role to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern. It is recommended that you refer to your organisation's policy on fraud when reporting allegations for further information on how you are protected.

When making a referral please provide as much information as possible, for example:

- the name of the person who you believe has committed a fraud;
- when and where the fraud has taken place;
- how long the fraud has been going on; and
- any details you have to substantiate your suspicion.

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 50 Cannon Street, London EC4N 6JJ. 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 Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited 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. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has 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.