Quarter 1
2016/17

Local Counter Fraud Specialists (LCFS)

Fraud Awareness Newsletter

Welcome

Welcome to this edition of the Fraud Awareness Newsletter.

We will provide an update on the latest NHS fraud cases and provide you with information on one of the latest scams. There are also helpful tips on "CEO fraud" and how to prevent it.

While the majority of people who work in or use the NHS are honest, fraud does exist and is a serious issue. Fraud in the NHS, on any scale, diverts resources from patient care and services. Your Counter Fraud team aims to make people aware that fraud is being tackled. Please see the contact details of the LCFS team overleaf.

In the News….

NHS computer specialist sentenced for eBay fraud

An IT specialist who stole equipment from a hospital and then sold it on eBay has been sentenced after an investigation by police and NHS fraud specialists.

Scott Gill, 39, pleaded guilty to an offence under the Theft Act (1968) at Doncaster Magistrates Court, South Yorkshire (1st April 2016) and must serve a 250 hour community order. He must also pay compensation of £5,000 to Doncaster and Bassetlaw Hospitals NHS Foundation Trust.

He was employed as an IT specialist by the Trust from September 2005. An anonymous tip off was received via NHS Protect's Fraud & Corruption Reporting Line.

Computer equipment was stolen and sold by Mr Gill on eBay

Further investigations revealed that the goods sold on eBay matched the serial numbers of computer equipment used by the Trust, some of which were reported stolen by Gill during an alleged burglary.

Mark Bishop, Counter Fraud Specialist at Doncaster and Bassetlaw Hospitals NHS Foundation Trust, said: "Hospital equipment is precious and should not have been abused in this way. This conviction will hopefully act as a deterrent to others who might consider stealing from the National Health Service".

April 2016

Drug addict heart doctor forged prescriptions

An NHS consultant who forged prescriptions in the names of family and colleagues to steal drugs has been sentenced at Liverpool Crown Court following a fraud investigation supported by NHS Protect.

Martin John Royle, 44, had earlier pleaded guilty to eleven offences – two of fraud and nine of Forgery and Counterfeiting. He was sentenced to four months imprisonment, suspended for two years, and must pay £6,405.

In September 2013, Royle was a consultant cardiologist at St Helens & Knowsley Teaching Hospitals NHS Foundation Trust on Merseyside. He wrote and submitted a prescription for Tramadol which was for his own use, but which named a colleague as the recipient without their knowledge.

The incident was reported, and resulted in an investigation which revealed that Royle had forged at least 11 other prescriptions, using the names of colleagues and family members as the patient.

Pauline Smith, Anti-Fraud Specialist at NHS Protect, said: "The NHS and its patients expect the highest standards of integrity and professionalism from its staff, and this behaviour fell well below those standards.".

February 2016

Need to Know...

CEO Fraud on the increase

There are warnings to be on high alert after increased reports and financial losses from CEO fraud.

How does this scam work?

CEO fraud will typically start with an email being sent from a fraudster to a member of staff in an organisation's finance department. The member of staff will be told by the fraudster, who is purporting to be a Director or a Chief Executive, that they need to quickly transfer money to a certain bank account for a specific reason. The member of staff will do as their bogus boss has instructed, only to find that they have sent money to a fraudster's bank account.

The fraudster will normally redistribute this money into bogus 'mule' accounts and then close down the bank account to make it untraceable.

Organisations are taking too long to discover that they have been the victim of fraud and the lost money has already being moved by fraudsters into mule accounts. Many organisations who suffered this type of fraud reported initially being contacted via emails with gmail.com and yahoo.com suffixes.

How can we protect ourselves:

- Ensure all staff, not just finance teams, know about this fraud.
- Have a system in place which allows staff to properly verify contact from their CEO or other senior members of staff; for example having two points of contact so that the staff can check that the instruction which they have received from their CEO is legitimate.
- Always review financial transactions to check for inconsistencies/errors, such as a misspelt organisation name.
- Consider what information is publicly available about the organisation and whether it needs to be public.
- Ensure computer systems are secure and that antivirus software is up to date.

Contact your Local Counter Fraud Team

Concerns about fraud?

Contact your Local Counter Fraud Specialists (LCFS) team in absolute confidence.

Neil Mohan

T: (0) 1509 604 029
E: neil.mohan@nhs.net

Juliette Meek

T: 01603 883099

M: 07802 658845
E: juliette.meek@nhs.net

Gina Lekh

T: (0) 1223 552333
E: g.lekh@nhs.net

Dominika Kortus

T: (0) 7730 146 627
E: dominika.kortus@uk.pwc.com

You can also contact the NHS confidential fraud reporting line on 0800 0284060 and www.reportnhsfraud.nhs.uk

Further details of all NHS fraud prosecutions can be found on the website of NHS Protect at: www.nhsbsa.nhs.uk/3378.aspx