



# Fraud Counts Newsletter

## International Fraud Awareness Week



### International Fraud Awareness Week – 15<sup>th</sup> to 21<sup>st</sup> November

2020 has been a highly unusual year for everybody and COVID-19 has forced almost everybody to work in different ways. One of the aims of our work is to raise awareness of fraud amongst staff groups. With this in mind and as part of International Fraud Awareness Week, we held a series of virtual fraud awareness sessions, covering cyber-crime, HR and Recruitment, Fraud Champions and Standards of Business Conduct, Procurement and Security inviting a guest to take part in an interactive session to explore and discuss the areas in more detail.

This newsletter feeds back some useful information from each of the sessions for organisations to take forward, some lessons learned, and how we propose to address more of the questions raised through future counter fraud briefings.



NHSCFA Copyright 2020 – This information is licensed under the terms of the Open Government Licence.

### Cyber-crime – special guests, Martin Price (Royal Cornwall Hospitals Trust) and John Cullen (NHS Counter Fraud Authority)



This Photo by Unknown Author is licensed under CC BY-ND

We touched on some of the technical responses to cyber-crime. The discussion confirmed that whilst these responses are highly effective at combatting cyber-crime, it is inevitable that some attacks get past firewalls, anti-spam software etc. This is because new threats can only be countered as the criminals create them. There are an estimated 560,000,000 phishing attacks every day so although only a very low percentage get through the technical defences, it still leaves staff as the last line of defence against a significant number of attacks.

The Webinar focussed on hackers increasingly moving to social engineering techniques to get their victims to divulge sufficient information to either successfully guess passwords or to con people out of the answers to traditional password reset questions.

We will be issuing more material to help staff identify when they are targeted by cyber-criminals. Some people will include information on social media pages that criminals find very useful and social media quizzes often include a small number of questions from which criminals can elicit password reset questions.

**Suspicious of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line  
in confidence - 0800 028 40 60 or [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk)**





## HR and Recruitment – special guests, Jodie Leonard and Cigdem Higgins (University Hospitals Bristol and Weston NHS Foundation Trust)



We considered the main fraud risks faced by our HR and Recruitment teams, including fake ID and false qualification frauds, frauds relating to sickness leave and abuse of position frauds. These risks are mitigated by ensuring staff are aware of Trust policies which include relevant fraud prevention guidance.

Since the start of the COVID-19 pandemic, Trusts have seen an increase in COVID-related frauds, including false claims for free accommodation and falsely representing symptoms. Some organisations within the region have reduced the likelihood of fraud attempts in this area in many different ways, a particularly pragmatic one being offering staff members with suspected COVID-19 symptoms an immediate test.

As part of next year's counter fraud activity, we plan to conduct a post COVID verification exercise which, in part will check the authenticity of qualifications, references and employment history in a sample of job applications. We will also offer guidance for HR teams and recruiting managers in relation to document checks.

## Fraud Champions and Standards of Business Conduct – special guest, Sarah Burns (Torbay & South Devon NHS Foundation Trust)

Standards of Business Conduct are particularly relevant to staff involved in the process of buying goods or services or involved in recruitment. We highlighted some of the more high-profile examples found in the NHS, particularly staff members outsourcing work to companies that they also own. Any member of staff could be offered gifts or hospitality from a potential supplier and the importance of complying with the organisation's own policies was emphasised. Monetary gifts from grateful patients and relatives were explored. In general, these should be refused but if this is not possible, they must be passed to the organisation's charitable funds office.

Fraud champions are a recent addition to the fight against fraud. This session helped affirm their value and, in particular, endorsed views that Fraud Champions may be a very good conduit for staff that may be daunted by the thought of speaking to a Counter Fraud Specialist.

As a result of this webinar, we are looking to form a SW Fraud Champions network. A future edition of Fraud Counts will concentrate specifically on this topic answering a number of questions raised around the role.



## Be a fraud fighter

Everyone has a part to play in fighting NHS fraud. Join us and read our latest advice at [cfa.nhs.uk](http://cfa.nhs.uk)



NHSCFA Copyright 2020 - This information is licensed under the terms of the Open Government Licence.

## Always report cyber incidents immediately

For work related cyber-crime such as suspicious emails via NHS Mail or work phone calls, contact your local IT departments. For cyber-crime incidents outside of work you can report to:

- **Action Fraud**—0300 123 2040
- **Phishing emails** – [report@phishing.gov.uk](mailto:report@phishing.gov.uk)
- **Spam texts** – 7726 (standard phone key pad – spells SPAM)



## Procurement – special guest, Mark Slaney (Torbay & South Devon NHS Foundation Trust)

**NHS**

**Remain vigilant to  
stop procurement fraud**

During emergencies like the COVID-19 pandemic, NHS procurement can become more vulnerable to fraud.  
You can help stop fraud – find out more at [cfa.nhs.uk](https://cfa.nhs.uk)

NHSCFA Copyright 2020 - This information is licensed under the terms of the Open Government Licence.

We explored standard procurement controls and the reasons for them being in place. The question, “Does the idea of not paying an invoice unless it quotes the appropriate purchase order number help reduce the risk of fraud?” Similarly, “Does the requirement for goods/services to be receipted before the payment is made help reduce the risk further?”.

The concept behind this is called “separation of duties” and means that no individual should be responsible for all stages of procurement.

The necessity for a purchase order number means that the appropriate procurement process is followed together with the checks and balances that are built into the process. The “goods receipting” stage gives assurance that the organisation has received the goods or services for which it is invoiced. Therefore, the requirement for quoting a purchase order number and formal receipting of goods does reduce the fraud risk considerably.

Issues around very newly formed and inexperienced companies supplying PPE to organisations was discussed and one example was quoted of a new company supplying 1,000,000 face masks to a hospital that were not of the type needed. In this case, fortunately, the hospital was able to return the masks and got their money back.

COVID has posed particular challenges to Procurement and the Government has encouraged public sector organisations to do what they could to help suppliers continue trading during the pandemic. The question was asked as to whether suppliers should be paid in advance. There was a consensus that in some circumstances, this may be appropriate but if there are any doubts, offering part payment in advance reduces the risks to the NHS.

Potential procurement frauds and how these can be mitigated will feature in a future edition of Fraud Counts.

**Fraud in Your  
NHS Workplace?**

**Report it!**

If you have any suspicions or concerns,  
You can call us anonymously on

**0800 028 40 60**

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information  
The NHS Counter Fraud Authority leads on fighting fraud, bribery  
and corruption in the NHS and the wider health group

**Counter Fraud Authority**

**Department  
of Health &  
Social Care**



## Security – special guests, Gary Thompson (Royal Devon & Exeter NHS Foundation Trust) and Matt Adams (University Hospitals Bristol and Weston NHS Foundation Trust)



This Photo by Unknown Author is licensed under CC BY-NC

COVID has altered the way in which the NHS works and this brings changes to the approach to security. Of particular interest were security risks with home working. This mainly centres on risks around Trust equipment being stolen from staff member's homes. This may either be through break-ins if equipment is left in view from ground floor windows, or perhaps a lack of monitoring of equipment taken home by staff which could find its way onto eBay. This also highlights the associated risk of data falling into the wrong hands.

The session explored the technological advancements assisting fraud/security work. Bodycam footage and constant improvement of CCTV quality is helpful in many Fraud and Security investigations, in order to identify those who decide to commit acts of violence, theft or fraud against the NHS. Door swipe access is of great importance to both Counter Fraud and Security, as access and egress from a building can be controlled and monitored remotely.

We were asked for advice on particular security/fraud trends during COVID and what could people do to protect themselves. Theft of PPE, whether through the security aspect of brute force attacks, or from a more fraudulent angle of PPE never arriving at NHS locations due to fraudulent suppliers or couriers was discussed. This equipment has become high value due to the pandemic and must be both procured and held securely.

We encourage managers to ensure they know what equipment staff have taken home and encourage staff to ensure that equipment is adequately secured together with any data held on any IT devices.

### Conclusion

These webinars are a successful and very safe way for your Counter Fraud team to interact with staff. If you would like to consider holding webinars within your organisations for discussion, information and learning to combat fraud, please contact your Local Counter Fraud Specialist, details are included below.




















In the meantime, we wish to publicly thank all our guests for sharing their knowledge and experience with us and making the webinars so successful.



## OUR LOCAL COUNTER FRAUD TEAM

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance ([www.aswassurance.co.uk](http://www.aswassurance.co.uk)), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact your Local Counter Fraud Specialist (LCFS) below.

	<p><b>Gareth Cottrell – Interim Counter Fraud Manager</b> 01872 258057 or 07814 002364 <a href="mailto:gareth.cottrell@nhs.net">gareth.cottrell@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> Royal Cornwall Hospitals NHS Trust</li> <li> Cornwall Partnership NHS Foundation Trust</li> <li> Cornwall Care</li> </ul>		<p><b>Tracy Wheeler - LCFS</b> 01752 431378 / 07789 868568 <a href="mailto:tracy.wheeler2@nhs.net">tracy.wheeler2@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> University Hospitals Plymouth NHS Trust</li> <li> Devon Partnership NHS Trust</li> <li> Livewell Southwest</li> </ul>
	<p><b>Shamaila Asghar - LCFS (maternity cover for Adele Rilstone)</b> 07775 417508 <a href="mailto:shamaila.asghar@nhs.net">shamaila.asghar@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> Torbay and South Devon NHS Foundation Trust</li> </ul>		<p><b>Alice Lee - LCFS</b> 07813 540022 <a href="mailto:alicelee1@nhs.net">alicelee1@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> Devon CCG</li> <li> Out of Hours Service Providers</li> </ul>
	<p><b>Eli Hayes – LCFS</b> 07920 284239 <a href="mailto:elias.hayes@nhs.net">elias.hayes@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> University Hospitals Bristol and Weston NHS Foundation Trust</li> <li> Bristol, North Somerset and South Gloucestershire CCG</li> </ul>		<p><b>Mo Jackson - LCFS</b> 07824 606899 <a href="mailto:mo.jackson@nhs.net">mo.jackson@nhs.net</a></p> <p>LCFS for:</p> <ul style="list-style-type: none"> <li> Northern Devon Healthcare NHS Trust</li> <li> Royal Devon &amp; Exeter NHS Foundation Trust</li> </ul>