NHS Counter Fraud Authority

# Circular

| | |
|---|---|
| **Circular reference** | G/04/2018-19 |
| **Publication date** | 27 July 2018 |
| **Subject** | **Fraud against suppliers of the NHS** |
| **Who should read** | Local Counter Fraud Specialists<br><br>Directors of Finance/Chief Finance Officers |
| **Action** | **LCFSs:** arrange dissemination to NHS procurement teams and to NHS suppliers<br><br>**DoFs:** for information only |

## Contents

# Summary

A number of NHS health bodies are being targeted as part of a procurement fraud. This fraud is being directed predominantly at existing suppliers providing goods to the NHS and suppliers not previously used by the NHS health bodies. The loss from the fraud is being suffered by the suppliers (there has been no loss to the NHS), however health bodies should take the necessary precautions to avoid falling victim to this fraud. The fraud presents a risk to the NHS if no action is taken and creates a potential for reputational damage.

We are issuing this advice to NHS organisations and their LCFSs so they are able to disseminate information to suppliers to make them aware of the fraud.

# Background

Suppliers that provide items such as equipment, consumables and medicines to NHS organisations are being contacted by unknown persons/third parties claiming to be employed or part of an NHS organisation (e.g. they claim to be working in the procurement team) and placing an order on behalf of the NHS organisation.

We are aware that one supplier has already been defrauded of around £62,000 worth of medical equipment before the fraud was discovered. Another supplier has been defrauded of around £25,000.

# How the fraud operates

A supplier is contacted via email and asked to provide quotations. They are also asked to confirm their settlement terms, i.e. whether they accept the standard 30 day payment terms after receipt of invoice. Many of the orders exceed £50,000 and are followed up with official looking purchase orders using the NHS logos, fictitious names, reference numbers and signatures. The expectation is that this order will slip through the system and the NHS organisation could end up paying for the goods.

Recently, there have been attempts to obtain goods in this way. The delivery addresses are non-NHS locations, such as business parks or warehouses. Due to the unusual delivery addresses, some suppliers have contacted the NHS organisation purchasing teams directly and have been advised of the fraud prior to the goods being shipped.

# What to look out for

NHS organisations should make their suppliers aware of this fraud and remind them of the following precautions:

- Check whether the correct email addresses are being used (i.e. a genuine NHS email address). They should be alert to suspicious looking email addresses and seek confirmation from the NHS organisation. Hover over or right-click an email address to check the properties. Genuine NHS emails normally end with ".nhs.uk" and do not contain ".com" or ".org".
- Check the general appearance of the email, such as greetings used (e.g. using generic Dear Sir/Madam rather than a named individual), spelling, wording/grammar, design or image quality.
- Undertake due diligence checks when purchase orders are received from a new contact. If you are suspicious, contact an established point of contact in the NHS organisation (i.e. an established contact in the procurement team).
- Check whether the delivery address on the purchase order is an NHS address. Fraudulent addresses will typically be a different address to the NHS organisation such as a domestic address, self-storage facility or unknown location/warehouse in the UK or overseas.
- Be wary of any later requests for changes or redirections to the delivery address. This should be validated by an established point of contact from the named NHS organisation.
- Ensure suspicious orders are verified with the relevant nominated individuals at the NHS organisation before accepting any orders. Do not use the contact details shown on suspicious emails.
- Set up a spam filter with the fraudulent email address that is being used so future and current communications can be monitored. This should be done with the help of the IT department.
- If in doubt do not process payments until you are satisfied that you are dealing with genuine NHS staff.

# Action

Action required by NHS organisations:

- Contact suppliers advising them of this fraud and remind them of the procurement procedures.
- Consider issuing an alert on your website to raise awareness of the fraud.
- Encourage suppliers to report incidents of suspected fraud to the police via Action Fraud, on 0300 123 2040 or through their online reporting tool.
- All incidents of suspected fraud against an NHS organisation should be reported to the nominated LCFS and the NHSCFA (by calling 0800 028 4060 or online at www.cfa.nhs.uk/reportfraud).

# Contact details

If you have any further queries about issues raised in this circular please email prevention@nhscfa.gsi.gov.uk.