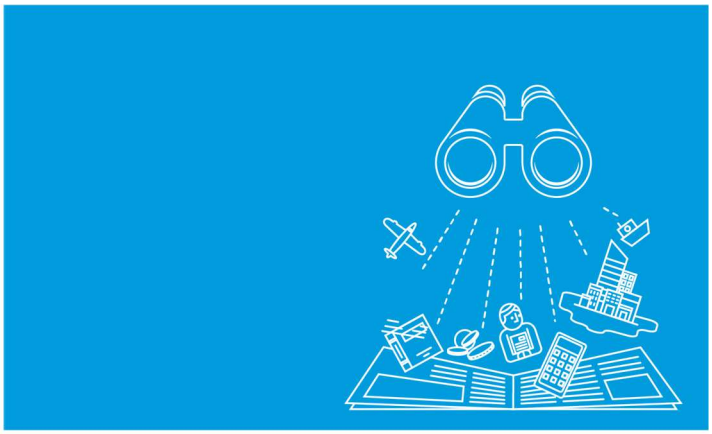
Invoice fraud spotlight



Invoice fraud is any deliberate deception intended to influence and stage of the purchase to pay cycle in order to make a financial gain or cause a loss. The purchase to pay cycle covers requisitioning, receiving, paying for and verifying the supply of goods and services.

Invoice fraud categories

There are three categories invoice fraud at a local level:

Insider fraud - this refers to cases of fraud in which an insider's access to the NHS organisation's assets and payments, or their ability to influence the outcomes of organisational processes, would be essential for committing the fraud.
Examples of insider fraud include:

- false payment requests;
- billing fraud, e.g. overbilling a debtor, or creating overpayments to creditors and pocketing the difference/refunds;
- procurement fraud, e.g. submitting false invoices for payment, or collusion with a supplier to have marked-up invoices submitted.

Supplier fraud - this includes any fraud for which it can be shown that steps were deliberately taken by the supplier to mislead a health body with a view to obtaining payments that were not properly due.
Examples include:

- duplicate invoicing;
- over-inflated commission;
- VAT fraud;
- invoicing for services not supplied.

Mandate fraud - this is also commonly described as 'change of bank account scams', 'payment diversion fraud' or 'supplier account takeover fraud'. This occurs when a fraudster purports to be from a supplier where regular payments are made to. The fraudster is successful in getting an organisation to change the payment details and successfully diverts future payments in order to gain financially. The details of suppliers are obtained from a range of sources including corrupt staff, publicly announced contracts and on-line logs of supplier contracts and expenditure publications.

Preventing and detecting

Establish the right culture. Setting the right anti-fraud culture within the health body is vital in preventing fraud and corruption. Ensure those involved in the process of payment of invoices comply with Standing Orders / Standing Financial Instructions, Standards of Business Conduct / conflict of interest requirements and the Anti-Fraud policy (or equivalent).

Skills and knowledge of staff. All executive directors, non-executive directors and staff should be aware of the organisation's anti-fraud and conflicts of interest policies. Training should also be provided to relevant staff on anti-fraud issues to ensure that staff are aware of those indicators which may require further enquiries to be undertaken.

Maintain a register of changes of suppliers' details. Appropriate contact should be made with the (real) supplier using original contact details to confirm any requested changes and then a bank account amendment form should be sent to their Finance Director or Company Secretary to sign, confirming the change of bank account details. A model amendment form is available from your Local Counter Fraud Specialist (LCFS)

Know your supplier. Suppliers should be asked to confirm information already held by the health body, such as the previous bank account details, registered address, email address, company registration number, company VAT number or the name of the Company Secretary.

Actively monitor the payment process. Continually monitor the internal control framework to ensure it remains effective. Undertake regular fraud risk assessments and internal audits to identify threats. It is recommended that health bodies undertake accounts payable audits to identify duplicate payments, incorrect supplier payments, missed discounts and rebates and tax errors.

Communication. Suppliers should be made aware, in writing, of your organisations' policy regarding changes to methods of payment bank account details, both at the time contracts are signed and through regular updates. Any genuine supplier will be happy to provide adequate notice of a mandate changes, and will comply with any instructions.

Beware of social engineering - this is the psychological manipulation of people and systems into divulging confidential information and performing actions that they otherwise wouldn't.

1. Fraudsters make initial contact via email to the NHS organisation's generic finance department mailbox, purporting to be from a contractor.
2. The email contains a common template with the contractor's name, logo, and genuine office addresses and requests information about the procedure to change bank account details for future payments.
3. A subsequent email is then sent to the contractor, purporting to be from the NHS organisation (using a fake email domain and email signature from the NHS organisation's finance department) to request any outstanding invoices due for payment.
4. This information is then used to gain the trust of the NHS organisation they are attempting to defraud and a convincing email, purporting to be from a genuine contracted supplier, is then sent to the NHS organisation, with a request to change bank account details.

The current pandemic has brought with it increased risks of fraud, particularly where organisations have had to relax some controls and staff have had to work remotely. These relaxed controls may be exploited by people inside and outside of the organisation, meaning additional vigilance is required. Some areas where risks may have increased include;

Invoice fraud
- Urgent payment requests exploiting Covid-19
- Relaxed segregation of duties
- Mandate change requests not easily being verified

Credit Cards
- Increased credit card spends
- Credit cards used by multiple individuals due to increased pressure
- Expenditures being reviewed retrospectively
- Non-essential or inappropriate purchases may not be identified promptly or easily attributed to an individual

Expenses
- Claims made for expenses which were not incurred
- Claims may exceed daily subsistence allowances
- Limited verification process to ensure prompt payment
- Staff may exceed the permitted allowances in meal and incidental charges

New supplier set up
- Urgent new supplier required to be set up, due diligence checks not carried out
- Relaxed segregation of duties

Your LCFS can provide more in-depth training showing examples of invoice fraud identified across the NHS which can be delivered face to face or online. If you wish to arrange a workshop, require any further information regarding fraud or bribery within the NHS, or have identified any concerns please contact your LCFS directly.

For further information please contact:

Kirsty Clarke
Senior Consultant

LCFS

020 3201 8054
kirsty.clarke8@nhs.net

kirsty.clarke@rsmuk.com