NHS
Counter Fraud Authority

Payment diversion fraud

Guidance for prevention and detection

July 2026 I Version 3.0

Working together to find, report and stop NHS fraud

Version Control

Version	Name	Date	Comment
1.0	Fraud Prevention Team	10/07/2018	
1.1	Fraud Prevention Team	18/02/2019	Title changed to reference mandate fraud. Changes made to sections 4 and 6 in line with updated guidance sent to NHS organisations on mandate fraud.
2.0	Fraud Prevention Team	31.10.22	Revised, updated and refreshed.
3.0	Fraud Prevention Team	30.04.26	Redrafted

Table of contents

1. Introduction

1.1 The NHS Counter Fraud Authority's (NHSCFA) 2025 Strategic Intelligence Assessment estimates that £392.5m of NHS funding is vulnerable to loss through fraud, bribery, and corruption from procurement and commissioning fraud, which includes payment diversion fraud.

1.2 This document provides Local Counter Fraud Specialists (LCFSs) and finance staff working in the NHS with guidance to support work to prevent and detect the most common kinds of payment diversion fraud at a local level. It introduces the subject area, provides an overview of the NHS payment and invoicing environment and offers practical advice on the most effective ways of tackling payment diversion fraud and how to report suspected fraud and corruption.

1.3 In accordance with government functional standard, Gov013, this guidance aims to assist LCFSs in identifying and assessing potential areas of payment diversion fraud risks within their organisations, so that local proactive exercises can be undertaken, where appropriate.

1.4 This guidance supersedes the previous invoice and mandate fraud guidance for prevention and detection.

2. What is payment diversion fraud?

2.1 Payment diversion fraud is a term that encompasses several common fraud types, including mandate fraud, chief executive officer (CEO) fraud, business email compromise fraud, invoice fraud, and insider fraud.

2.2 Payment diversion fraud involves fraudsters creating false invoices, making requests for payment or altering payment instructions, to divert payments into their own bank accounts. Fraudsters often monitor, hack, or spoof (copy) email accounts to impersonate a known and trusted entity, e.g. a supplier or senior staff member, to defraud the NHS organisation.

2.3 Fraudsters will often target finance, payments or payroll staff, and may use urgent, high-pressure tactics to convince the staff member to update bank details for a payment to be made.

2.4 This type of fraud exploits trust and weaknesses in verification processes, making strong cyber security, multi-factor authentication, and rigorous validation of bank detail changes essential to prevent financial loss and disruption to NHS services.

2.5 Good governance is also essential, and NHS organisations should have in place internal policies and standing operating procedures (SOPs) for their staff to adhere to, in particular those processes for **managing conflicts of interest** to safeguard against manipulation of controls and systems to change payment details.

3. Mandate fraud

How the fraud occurs

3.1 Mandate fraud is a common type of payment diversion fraud that occurs when someone attempts to get an organisation to change a direct debit, standing order, or bank transfer mandate, by claiming to be from a supplier they make regular payments to, to receive unauthorised payments.

3.2 The fraudsters may identify regular supplier payments that are made to NHS organisations through corrupt staff, monitoring public records of contracts, social media, or hacking company email accounts. Fraudsters will then contact the NHS organisation via email, phone/video call, or letter, impersonating a legitimate supplier or senior employee.

3.3 They will claim their bank details have changed and provide new account information. The request often highlights an urgent need for payments using social engineering techniques (see below), often during busy periods, for example year-end, or summer holidays to trigger quick compliance.

3.4 Once the bank mandate is updated, subsequent payments are diverted to the criminal's bank account unnoticed.

Prevention

3.5 NHS organisations should ensure that robust authorisation and monitoring procedures are in place for changing bank details as follows:

- staff should always independently verify requests to change supplier details by using the established contact details already held on file. They should ensure these details have not been subject to recent change (which may be requested as a precursor to a fraud being committed)
- it is important that staff corroborate the details held on file, e.g. by checking the supplier's official website, to ensure that they are accurate
- if a call from an alleged supplier seems suspicious, staff should note the incoming number and call back using established contact details held on file
- staff should check the authenticity of any email request received from a supplier, in particular noting if there are subtle changes to the domain name, by using established supplier contact details already held on file
- the supplier's contact details should be taken from existing records held by the NHS organisation and not from information supplied in the change request
- raise staff awareness of social engineering techniques used by hackers to commit payment diversion fraud
- as an extra layer of protection dependant on risk, when a request to change a bank account is made, ask the supplier to complete a bank account amendment form, signed by their finance director or company secretary, confirming the change of bank account details. **See example form in Annex A**. Consider also asking the supplier to confirm the amount and date of their last three transactions
- information provided on the returned amendment form should be checked

against the NHS organisation's existing records before any change is made

Process

- SOPs should be in place for finance and spending department staff involved in the payment processes, from raising a purchase order, invoice checking, authorisation and payment run. Instructions should cover actions for staff to take when suspicious activity is suspected, such as immediate reporting and putting a freeze on payments
- training should be provided to staff on an ongoing basis, to be aware of mandate fraud and how to verify a telephone/video call, letter or email request to set up a new or amend existing payment instruction
- there should be regular communication with suppliers to emphasise their shared responsibilities to protect against mandate fraud, such as strengthening cyber security (e.g. data security), updating devices with the latest cyber security software and anti-virus updates, and training staff on how to recognise and prevent cyber-attacks
- review and assess how much information is made publicly available and how it could be used against the organisation
- to verify proposed new bank account details, use a Confirmation of Payee function, a real time check that makes sure the name on the bank account matches the intended payee. Question where the bank account does not match the supplier name
- ensure segregation of duties and appropriate levels of access with respect to invoice processing tools in payment systems

Social engineering

3.6 Social engineering is the psychological manipulation of people into divulging confidential information and performing actions that they would otherwise not normally do. NHS organisations should be aware of how perpetrators use social engineering techniques to commit fraud.

3.7 A fraudster will typically contact the NHS organisation payroll or finance staff by email, phone, or increasingly by video call, impersonating an NHS organisation employee or a legitimate supplier. They will gain their trust by using genuine information about the employee or supplier to manipulate finance and payroll staff into changing bank account details or making immediate payments.

3.8 Red flags to look out for:

- requests by email, phone, video call or letter suggesting that there is an urgency in making the change of account details and processing payments due
- emails that impersonate a legitimate person or supplier, but domain names may have been altered slightly to appear legitimate. The email may contain other subtle differences such as poor grammar, a change in language from formal to informal, and the pressure of urgency to make the payment
- the email persuades the staff member to do the wrong thing such as click on a link or attachment that downloads malware, visit a website to enter personal details used to clone someone's identify, or to make immediate payments or bank transfers

4. Invoice fraud

How the fraud occurs

4.1 Invoice fraud is a key component of payment diversion fraud, whereby a fraudster submits fake invoices to obtain payments that were not properly due. Invoices may be submitted through compromised email accounts or letters requesting payments to be made into the fraudsters bank accounts.

4.2 Poor controls heighten the risk of invoice fraud. Where invoices do not provide a full breakdown of the amount due, it is difficult to determine whether the correct amount has been paid. There are also increased risks by not having systems in place to check that the invoice amounts are correct and there are no hidden or incorrect fees, that charges made against the contractual arrangements are accurate, and that the goods and service being billed were purchased and have been supplied.

Prevention

4.3 To prevent invoice fraud the following important controls need to be in place:

- Standing Financial Instructions (SFIs) should detail all the essential information that invoices should include to enable checks that payments are valid and correct
- information on invoices should be the same as supplier details already held on file. Checking previous bills received from the supplier, and that invoices have not been altered or are incomplete helps to reduce the fraud risks
- NHS organisations should check invoices to ensure they do not include duplicate payments, incorrect supplier details and payments, missed discounts, 'hidden fees' (such as 'handling fees', 'on costs' and 'administration fees'), missed rebates, and VAT/tax errors
- invoices should be checked against the contractual terms to ensure that payments only relate to specified goods and services, and are charged at the correct rate
- spending reports with budget holders should be reviewed to ensure transactions and payments are as expected and any anomalies spotted and investigated further
- scrutinise purchase orders or booking confirmations, against goods and services received, and ensure that they match the invoices and payments made
- payment systems that identify duplicate invoices should be a standard control
- checks are needed to ensure VAT numbers are valid. An EU VAT number (including the UK) can be checked on-line: **Vies on-the-Web - European Commission**

Process

- clear SOPs for all finance staff involved in the invoice payment process, and including budget holders as appropriate

- the organisation should provide ongoing training to designated staff to assist them in the verification of invoices
- staff should only approve invoices in accordance with their NHS organisation's SFIs and associated schemes of delegation

5. Business email compromise fraud

How the fraud occurs

5.1 Business email compromise (BEC) involves cybercriminals takeover of a genuine account of a NHS organisation's employee, or that of a trusted supplier to commit fraud. They use a compromised email account that has been hacked or spoof a genuine email account and send it to an employee to trick them to transferring funds or revealing sensitive information.

5.2 BEC will use convincing looking emails, that might request unusual payments or contain links to fake websites to capture personal information/log in credentials and passwords. Emails may contain viruses disguised as harmless attachments, which are activated when opened.

5.3 Unlike standard phishing emails that can be sent out indiscriminately to millions of people, BEC attacks target specific individuals, and can be even harder to detect.

Prevention

- staff should avoid clicking links, attachments or replying to suspicious emails, even 'unsubscribe' links can be a trap
- be alert to emails demanding immediate action, threatening account closure, asking for financial information, or indicating a business account has been opened
- be mindful that junk email inboxes can contain harmful links and attachments, ensure they are checked regularly, and emails are deleted if not of use
- staff should be encouraged and advised on the creation of strong, memorable passwords for different systems, and system logins that lock after several failed attempts. Further guidance on strong passwords and how to stay secure online is available via the **NCSC: Three random words**
- multi-factor authentication (MFA) requires users to provide two or more verification factors to access an account, and using MFA can significantly reduce the risks from compromised passwords being used to commit BEC fraud

Process

5.4 NHS organisations should refer to the **National Cyber Security Centre's (NCSC) '10 steps to cyber security'**, in particular:

- take a risk-based approach to this fraud risk to secure data and systems
- ensure cyber security policies are fit for purpose, endorsed by senior leaders, and are communicated effectively across the organisation
- ensure employees are equipped to manage cyber security within their own environment by raising awareness of this fraud risk and providing training as necessary to employees in identifying and managing incidents

- provide clear reporting lines for suspicious emails to their IT and/or fraud teams

6. Chief executive officer fraud

How the fraud occurs

6.1 Chief executive officer (CEO) fraud is similar to BEC fraud, however in this instance fraudsters and cybercriminals impersonate an organisation's senior employee, e.g. CEO or director of finance to request a payment is made, often as a matter of urgency, into a bank account, defrauding the NHS organisation.

6.2 Fraudsters will focus on staff who have access to financial systems, payroll or personal information, impersonating a senior executive to trick them into performing money transfers or disclosing sensitive data.

6.3 Fraudsters will also make requests utilising previously compromised email accounts and employing social engineering tactics and techniques. Emails often use name spoofing, using the correct name of the senior employee but a slightly different email address.

6.4 Criminals are increasingly using AI technology to clone voices or create deepfake videos to impersonate individuals, such as CEO and directors of finance, to trick staff into authorising fraudulent payments or used to gather personal information that can be used for fraudulent purposes.

Prevention

6.5 To prevent CEO fraud the advice is consistent with BEC fraud. In particular:

- ensure automated information provided by finance team's generic mailbox does not reveal personal/team contact details which can be used to facilitate social engineering techniques with staff
- fraudsters can make an email appear to be from a genuine contact, such as a supplier or someone within your own organisation. Finance staff should be vigilant to social engineering indicators from email addresses purporting to be a senior member of the organisation
- red flags in the emails may include:
  - subtle changes to emails and domain names
  - unusual forms of address to the recipient and signature activity
  - referencing people's names who are not known
  - subject of the email having no correspondence to business activity
  - persistence of the emails
  - alert messages that may sometimes appear within the email
  - invoices should be scrutinised, and due diligence checks conducted on the information held already on a supplier on file (see invoice fraud section above)

Process

- finance and payroll staff should understand the risks of CEO fraud and know what

to look for when administering change requests and requests for payment

- an employee bank account change request form should be used, accessed securely online through the NHS organisations internal sites. Blank change forms should never be emailed to the person making the request
- deliver awareness raising to finance teams, and disseminate prevention advice, guidance, and recommendations on how to prevent CEO fraud, what to look out for, and where to report incidents
- support conversations between counter fraud, finance, and IT security departments to develop a collaborative organisational approach to ensure IT security, systems, software that can identify phishing and spoofed emails are up to date

7. Insider fraud

How the fraud occurs

7.1 Insider fraud involves individuals gaining access to the NHS organisation's assets and payments or influencing the outcomes of organisational processes that are used to commit payment diversion fraud. An insider refers to an employee, contractor or individual with legitimate access to the organisations systems.

7.2 Examples of insider fraud include:

- false payment requests: an insider using false authorisations for payment, submits a false invoice. They may take advantage of the time pressures and high volume of processing which typically occurs during book closing to approve invoices by the end of financial periods
- billing:
  - an insider overbills a debtor and pockets the difference
  - records false credits, rebates or refunds
  - creates fictitious suppliers and, or shell companies for fraudulent payments into accounts they control
- procurement:
  - an insider colludes with a supplier to submit marked-up invoices
  - alters legitimate purchase orders
  - falsifies documents or forging signatures to obtain authorisation for payment
  - submits false invoices for payment from fictitious suppliers into their own bank accounts
  - makes improper changes to supplier payment terms or other supplier details

Prevention

7.3 To prevent insider fraud include the following:

- ensure appropriate **due diligence checks are undertaken** on new and existing suppliers
- maintain an up-to-date list of authorisers, keep a list of starters and leavers, and

remove authorisers that are no longer in post

- keep disbursement information safeguarded from loss or destruction
- regularly review and remove as appropriate any unused suppliers still active on payee list after a set period
- monitor any bank details changes on a supplier's account, including any that are inactive and has not conducted work for a substantial period
- keep procedures covering the granting and removal of appropriate access rights to users, e.g. based on levels of seniority, appropriate to job roles, controls around time period/duration of access
- have clearly defined budget holders for all accounts

Process

- ensure systems and processes for managing conflicts of interest are reviewed and kept up to date
- maintain segregation of duties and ensure appropriate levels of access with respect to invoice processing in payment systems
- have in place whistleblowing training and clear reporting lines
- counter fraud training and awareness of insider fraud indicators to staff groups involved with processing payments
- have in place SOPs for all staff with responsibility for setting up and making creditor payments
- employment checks on new and existing staff to ensure that NHS organisations are making an informed decision when recruiting staff. Checks include verifying identity, employment history, references and criminal records. See NHS employer's guidance on employment checks: **Employment standards and regulation | NHS Employers**

8. Local proactive work

8.1 NHS organisations, based on their local risk assessments, should consider local proactive exercises around the payment control environment. This helps to pinpoint any weaknesses in controls and to develop actions plans for improvement. It also helps identify anomalies that warrant further investigations to detect fraud.

8.2 As part of proactive work, control testing can help assess how robust policies, processes and systems are, measures compliance with SOPs, and assesses how effectively suspicious requests are managed, reported and escalated, for example:

- assessing a finance team's response to a fictitious supplier request (e.g. phone, email, video call) to make a bank account change to divert funds into an altered supplier's bank account
- assessing a finance team's response to a fictitious senior employee (e.g. email, phone, video call) making an urgent payment or money transfer request into a designated bank account

9. Raising awareness of payment diversion fraud

9.1 NHS organisations should ensure that payment diversion fraud forms part of local fraud awareness initiatives and campaigns and LCFSs should support this initiative. This applies particularly to any events such as induction, awareness raising and ongoing training delivered to staff.

9.2 NHS organisations should ensure that staff with responsibility for making changes to bank accounts, processing and paying or authorising invoices, or for supervising these processes, are made aware of the risk of payment diversion fraud in line with the NHSCFA's guidance and intelligence publications.

9.3 The NHSCFA recommends that NHS organisations regularly communicate with suppliers of their collective responsibility to prevent payment diversion fraud.

9.4 Resources to support LCFSs in delivering local fraud awareness initiatives are available on the NHSCFA's website: **Fraud awareness toolkit**

10. If payment diversion fraud is suspected

10.1 If payment diversion fraud is suspected, the NHS organisation's escalation process must be followed. Immediate action is necessary to recover the NHS funds. It must be reported straight away to the LCFS and director of finance who will contact the NHS organisation's bank and advise them of the suspected payment diversion fraud. The NHS organisation's bank should be instructed to immediately contact the bank where the fraudulent transfer of NHS funds has been made and request an immediate suspension/freeze on the funds transferred into the suspected fraudsters' account.

10.2 Any further transactions should be suspended at once and the NHS organisation's escalation process followed.

11. Reporting payment diversion fraud

11.1 If a payment has been made in error due to fraud, it must be reported immediately to the NHSCFA's Financial Investigation team, **financialinvestigation@nhscfa.gov.uk**. Include details of the fraudulent bank account involved and, if available, the NHS fraud case management system (Clue) incident or investigation reference numbers. Recovery of funds can be challenging, but notifying the NHSCFA immediately helps to ensure the right approach is taken to support the recovery of funds.

11.2 The LCFS should report the incident on Clue as soon as possible, to enable the NHSCFA to use this reported intelligence to issue alerts and instructions about any suspicious/fraudulent bank accounts that have been compromised and any immediate solutions. The NHSCFA shares this with other NHS organisations to enable them to put in place suitable prevention measures and block any further frauds involving those compromised bank accounts.

12. Media relations

12.1 Proactive engagement with the media remains an excellent and cost-effective way to reach large public and NHS audiences with a deterrent, anti-fraud message. Tv and radio stations, newspapers and health trade titles have all shown a keen interest in payment diversion fraud given the potential scale of losses. The NHSCFA's corporate communications team offers a full communications and media liaison service so please keep us updated on any developments where we can support you. They can provide you with support and guidance to maximise opportunities to promote successes internally and externally both nationally and locally. At a local level, this should be led by health body communications teams, giving full support to their LCFS.

12.2 Contact the NHSCFA's corporate communications team if you have any communications enquiries: **comms@nhscfa.gov.uk**; and **media@nhscfa.gov.uk** for media enquiries.

Annex A – Example bank account amendment form

SUPPLIER INFORMATION		
Supplier's name:		
Registered address:		
Town:	**City:**	**Postcode:**
Telephone number:		
Email address:		
Remittance address (if different from above):		
Telephone number:		
Email address:		
Name of company secretary:		
Company registration number:		
Company VAT number:		

CHANGE OF BANK ACCOUNT	
Current details	
Name of bank:	**Account name:**
Account number:	**Sort code:**
New details	
Name of bank:	**Account name:**
Account number:	**Sort code:**

DECLARATION			
I declare that the information I have given on this form is correct and complete.			
Request completed by (print full name):			
Signature:			
Date:			
*** Please indicate using an X**			
Finance Director		**Company Secretary**	

To enable us to deal with your request please return this form as soon as possible to:
Details of NHS organisation:

NHS Counter Fraud Authority
10 South Colonnade,
Canary Wharf,
London,
E14 5EA
Tel: 0207 895 4500

www.cfa.nhs.uk