NHS
Counter Fraud Authority

Mandate fraud

NHS fraud prevention quick guide v1.0 July 2019

Mandate fraud is described as change of bank account scams, payment diversion fraud or supplier account takeover fraud.

What is mandate fraud?

Mandate fraud occurs when someone contacts an NHS organisation with a request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier that regular payments are made to. If the organisation accepts the fraudulent request, the payments are then diverted into the criminal's bank account. The genuine supplier details are usually obtained from a range of sources including corrupt staff, publicly announced contracts and online logs of supplier contracts.

CEO email fraud

CEO (Chief Executive Officer) email fraud is another form of mandate fraud whereby the fraudster requests changes to payroll bank account details. This type of fraud typically occurs when an email from a fraudster is sent to an NHS organisation purporting to be the organisation's CEO or a senior director with instructions to change bank account details of the person they are impersonating. The fraudster will request that funds are transferred as a matter of urgency to the alternative bank accounts. The member of staff receiving the email will feel pressured to comply due to the apparent seniority of the sender and urgent nature of the email.

Who is this quick guide for?

This guidance is intended for those staff working in NHS finance and payroll teams, particularly those responsible for setting up bank account details and processing bank payments.

How to spot mandate fraud

Mandate fraud can occur in different ways,

here are some methods to be aware of:

- A telephone request is received where the caller is suggesting some urgency in making a change to supplier's bank account details.

- An email request is received from an unknown email account that is not recorded on the NHS organisation's records.

- An email is received where a minor amendment has been made to the sender's address details, giving the impression it is a correct and genuine contact email address at first glance. For example, the genuine address is Joebloggs**363**@mail.com but the fraudulent email came from Joebloggs**36**@mail.com. Staff should always check the authenticity of an email received from a supplier (e.g. the domain name) by using established supplier contact details already held on file.

- A written request is received in the form of a letter or invoice that does not contain the supplier's logo or the logo may be less sharp or slightly blurred (this would most likely be a scanned copy of an original document which has been counterfeited).

How to stop mandate fraud

Controls that mitigate the risk of mandate fraud should be documented in a policy and standard operating procedures (SOPs) and staff should be trained on identifying and reporting any risks and breaches. Without proper controls, NHS organisations are at risk of unintentionally paying a supplier's invoice into a fraudster's account.

The following controls should be in place:

- NHS organisations should periodically confirm supplier information held on file including: previous bank account details, registered address, email address, company registration number, company VAT number or the name of the company secretary.

- When contacting a supplier this should be done using the supplier's contact details found in existing records held by the NHS organisation and not from information supplied in a change request.

- If there should be a need to amend bank account details, suppliers should be sent a bank account amendment form for their finance director or company secretary to sign, confirming the change of bank account details. Information provided on the amendment form should be checked against the health body's existing records before any change is made.

- A senior member of the finance team should always review any change of bank account details and formally authorise this.

- All staff should be aware of and adhere to internal procedures and controls to minimise the risk of losses to this type of fraud.

- There should be a segregation of duties and an appropriate level of access with respect to accessing invoice processing tools in payment systems.
- Staff should be vigilant for invoices related to office supplies as this is a known high risk area relating to all reported mandate fraud in the NHS.
- A dual control procedure for authorising payments should be implemented.
- Staff should be vigilant during the months of August and December, as analysis indicates these are vulnerable periods for mandate fraud to occur in the NHS.
- It is very important to maintain the organisation's processes around fraud prevention and treat it as a 'business as usual' activity.
- Staff should be clear about when and where to report all incidents or threats of mandate fraud.
- Staff should be trained on social engineering[1] techniques that can be used by an attacker to commit mandate fraud.

The signs of how to spot and preventative advice on how to stop CEO email fraud are very similar to those in mandate frauds. It is important that payroll staff are acutely aware of these risks when administering employee payroll banking account information.

If you suspect mandate fraud

- If a call from an alleged supplier seems suspicious, hang up and call the supplier organisation using established contact details held on the NHS organisation's records.
- If you suspect that a mandate fraud has occurred, the organisation's escalation process should be followed and immediate action is crucial and may prevent any actual loss of NHS funds. Staff must act immediately by alerting their Local Counter Fraud Specialist (see also how to report fraud below) and the following actions must be taken:

[1] Social engineering refers to the psychological manipulation of people and systems into divulging confidential information and performing actions that they otherwise wouldn't.

1. Your organisation's Local Counter Fraud Specialist or Director of Finance should contact the targeted NHS organisation's bank advising them of the suspected mandate fraud in action.

2. The NHS organisations bank should be instructed to contact the bank of the suspect account where the fraudulent transfer of NHS funds have been made to.

3. An immediate freeze on the funds should be requested.

How to report fraud

Report any suspicions of fraud to the NHS Counter Fraud Authority online at **https://cfa.nhs.uk/reportfraud** or through the NHS Fraud and Corruption Reporting Line **0800 028 4060** (powered by Crimestoppers). All reports are treated in confidence and you have the option to report anonymously.You can also report fraud to your nominated Local Counter Fraud Specialist.

Why take action?

By increasing scrutiny, embedding control measures and implementing fraud prevention action concerning mandate fraud, NHS organisations will reduce the associated risks and the potential for significant monetary losses.

Reporting incidents of mandate fraud, even unsuccessful ones, to the NHS Counter Fraud Authority will assist in the identification of individuals who are targeting the NHS and their methods for investigative action.

Further information

- **https://cfa.nhs.uk/fraud-prevention/fraud-guidance**
  - » Invoice and mandate fraud
  - » Pre-contract procurement fraud and corruption
- For further information visit the NHSCFA website **www.cfa.nhs.uk**
- Details of your Local Counter Fraud Specialist:

Space for business card / contact information