NHS
Counter Fraud Authority

Mandate fraud

NHS fraud prevention quick guide **v2.0 October 2022**

Mandate fraud is also known as payment diversion fraud, change of bank account scam, or authorised push payment fraud. Mandate fraud will often be cyber enabled, committed through the use of Information Technology (IT).

What is mandate fraud?

Mandate fraud occurs when someone contacts an organisation with a request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier that 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 email interception, corrupt staff, publicly announced contracts, and online logs of supplier contracts. Social engineering is a significant part of the cyber enabled mandate fraud process. Cyber criminals will pose as trusted and recognised people and use a sense of authority and urgency to manipulate individuals into making a bank transfer or providing confidential information.

This type of fraud is continuously evolving with cyber criminals becoming ever more sophisticated, increasing their ability to conduct cyber-attacks on the NHS. The vast majority of cyber enabled mandate frauds now relate to the hacking of emails, either NHS or supplier email accounts, or the use of copycat domain names.

Conversation hijacking: Cyber criminals will stealthily observe the pattern of work of the organisation, and review emails being sent. Once an interesting or valuable transaction is identified, the cybercriminals will tamper with the mail account settings, so the legitimate mail owner is unaware that their emails are being redirected to an obscure location or deleted. The cyber criminals may spoof the email with a false email address and request that bank account details are changed before requesting that further payments are made into the fraudsters bank account. This is done without the knowledge of the mail owner.

Business Email Compromise (BEC)

In BEC attacks, also known as CEO fraud, whaling, and wire transfer fraud, scammers impersonate

an organisation senior employee in order to defraud the target. In most cases the attackers will focus their efforts on those with access to financial systems or personal information, tricking individuals into performing money transfers or disclosing sensitive personal data. These attacks often make use of previously compromised accounts and utilise social-engineering tactics and techniques. The emails often do not include the usual attachments or links associated with malicious emails as the attacker is already within the organisation's email environment.

Who is this quick guide for?

This guidance is intended for those staff working in NHS finance, procurement, and payroll teams, particularly those responsible for setting up bank account details and processing bank payments and IT Security Teams who will be required to action certain prevention solutions suggested.

How to spot mandate fraud

Cyber enabled mandate fraud can occur in different ways, here are some methods to be aware of:

- An email request is received from an unknown email account that is not recorded on the NHS organisation's records.
- An email request is received purporting to be from the organisation's CEO or a senior director instructing the change of bank account details.
- 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 Joebloggs363@mail.com but the fraudulent email came from Joebloggs36@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.
- The email itself may contain poor grammar, a change in language from formal to informal, and pressure of authority or urgency to make the payment.

Hacked accounts email flow rules are being changed by cyber criminals in order that they are copied into all future emails that are sent between NHS organisations and their suppliers. This is achieved by using a fraudulent email address/domain name and creating a very similar one with a subtle difference which can be very difficult to spot.

Staff should be aware that for any mandate change requests, the email address/domain name may appear to match the one held on file, however this does not in itself make the request legitimate.

How to stop mandate fraud

Organisations should have procedures in place that detail a strong suite of controls to assist in preventing mandate fraud 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:

- Ensure that local IT security teams have protected the email accounts of staff in finance and procurement roles using techniques such as Two Step Verification (2sv). This helps prevent password theft from finance staff, which the cyber criminals then use to send misleading emails. Turn on 2-step verification (2SV) – NCSC.GOV.UK

- Staff are required to use Confirmation of Payee services. Any suspicions should be flagged with a supervisor before a transaction is made.

- Local finance teams should use Bankline for bulk payments.

- NHS organisations should undertake periodic reviews of the supplier database to weed out expired or obsolete records.

- When contacting a supplier to confirm a mandate change request 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.

- Fraudsters may request that contact details held on file are amended first, as a precursor to an attempted mandate fraud, it is important to check that details held on file have not been subject to recent change.

- If there is 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, signatures must be verified, confirming the change of bank account details. Information provided on the amendment with the date and value of the last payment made to the supplier form should be checked against the health body's existing records before any change is made.

- A senior member of the finance team (Deputy Director or Director of Finance) should review all change of bank account details and formally authorise this.

- There should be a segregation of duties and an appropriate level of access with respect to accessing invoice processing tools in payment systems.

- Where finance teams are able to procure external Bank Account Verification / Confirmation of Payee banking services, they may do so in order to reduce payment processing errors, reduce the risk of internal and bank transfer fraud.

- Cybercriminals may try to obtain access to accounts, by attempting to direct staff to a fake site that looks like the legitimate one in order to steal login/password details. Never click on the link or attachment from suspicious emails.

- Finance staff should create strong, separate passwords (using a combination of alphanumeric and special characters) and storing them safely without sharing is a good way to protect yourself online.

- Staff should be trained and frequently updated on fraud awareness and social engineering techniques[1] that can be used by an attacker to commit mandate fraud.

If you suspect mandate fraud

- If a call or email from an alleged supplier seems suspicious, take a note of the incoming number and/or email address, do not respond and call the supplier organisation using established contact details held on the NHS organisation's records. Ensure the details held on file are correct and have not been subject to an earlier attack.

- 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 (LCFS) (see also 'How to report fraud', below) and the following actions must be taken:

  - Your organisation's Finance team or Director of Finance should contact the targeted NHS organisation's bank advising them of the suspected mandate fraud in action.

  - The NHS organisation's bank should be instructed to contact the bank of the suspect account where the fraudulent transfer of NHS funds has been made to request an immediate freeze on the funds

  - Staff should report immediately to the Trust's LCFS who will contact the NHSCFA's financial investigators by emailing financialinvestigation@nhscfa.gov.uk. The NHS Wales LCFS will contact NHS CFS Wales Head of Counter Fraud or NHS CFSW financial investigators.

- IT departments should preserve all related data logs, analyse data logs, prepare an intelligence package, and refer for investigation.

- A post incident review/debrief is recommended to take place with LCFS, finance/payroll and IT security, to coordinate a joint risk assessments and remedial action.

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

How to report fraud

- Report any suspicions of general fraud to the NHSCFA 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 Trust's LCFS.

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 NHSCFA will assist in the identification of individuals who are targeting the NHS and their methods for investigative action.

Further information

- NHSCFA's fraud prevention guidance
- Invoice and Mandate Fraud Guidance
- Pre-contract Procurement Fraud and Corruption Guidance
- COVID-19 counter fraud guidance
- NHS Fraud Reference Guide
- For further information visit the NHSCFA website www.cfa.nhs.uk
- National Cyber Security Centre - NCSC.GOV.UK
- Contact your Local Counter Fraud Specialist for further detail