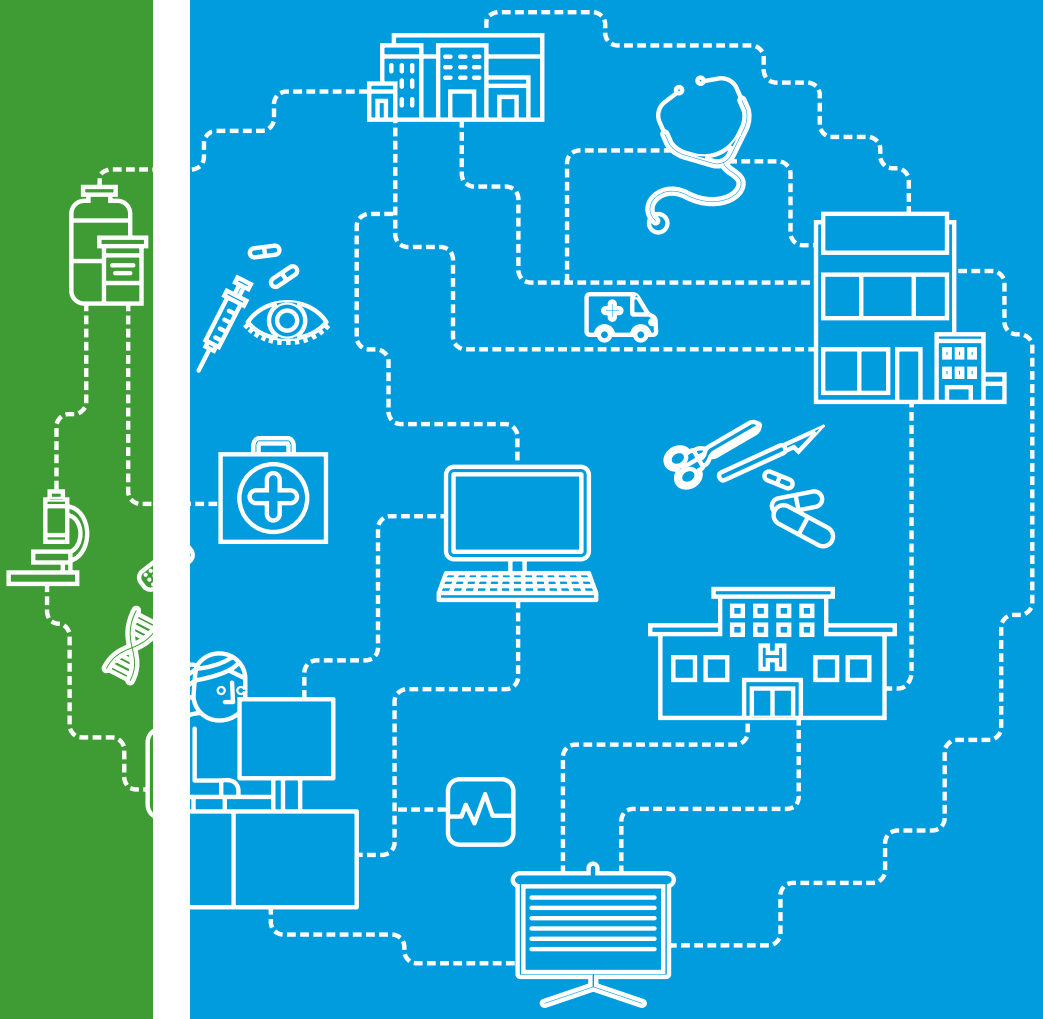
Mandate Fraud

Enhancing your defences



September 2022

Mandate fraud

Mandate fraud is where you are tricked into changing details of a direct debit, standing order or bank transfer from an individual or group who are pretending to be an organisation you make regular payments to. Mandate fraud also occurs where an invoice is received containing the incorrect payment details. It's a simple but effective fraud, used by organised crime and “career fraudsters”, as a low cost and low risk way to make money and to fund other types of criminality.

In accordance with NHS Counter Fraud Authority (NHSCFA) requirements, RSM’s NHS clients report all attempted mandate frauds. In 2021/22, reported mandate fraud attempts across our NHS clients reached over £6.4m. Whilst the risk of receiving a mandate fraud attempt is very high, the hard work, vigilance and the controls in place across the NHS, reduce the likelihood of an attempt becoming successful.

In this briefing we highlight common characteristics of mandate fraud, set out your key defences, and what you should do if you spot a possible mandate fraud attempt.

YOUR KEY DEFENCES

First line of defence

NHS staff are the first, and most valuable, key control to circumvent the risk of mandate fraud. When staff are aware of the risks, they are alert to attempts and with guidance and training, can spot the methodologies used by criminals, preventing public money being lost. Staff should be encouraged to attend finance or cyber-crime fraud related training offered by your Local Counter Fraud Specialist (LCFS).

Confirmation of account holder

Organisations should use the bank account verification system if available, before processing any new supplier payments or mandate changes. This system verifies the intended sort code and account number against the name of the intended payee and will only allow a payment if they are a match. This is not always available on BACS but organisations could consider a test transaction or verification without sending funds using CHAPS or Faster Payment systems.

Good cyber security

Criminals use various methods to gather key information, laying the groundwork to enable a mandate fraud attempt to more likely succeed. Initial activity can include hacking or putting malware into IT systems, particularly email systems.

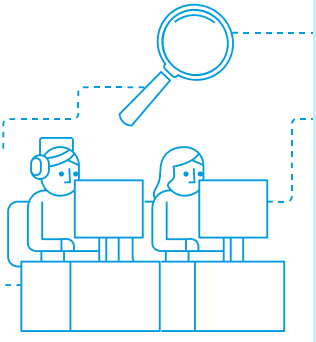
We have seen instances of fraudsters:

- “lurking” in NHS email accounts, monitoring the communication style and types of contacts;
- adding Outlook rules to divert emails, then sending emails purporting to be the genuine account holder which are then immediately deleted; and
- using “rules” to hide the responses from the genuine user.

This allows the fraudster to have a full email conversation with the intended victim from a genuine company email account.

Yet, this risk is not limited to NHS systems. Fraudsters will often target an NHS supplier, in order to gain control of an email chain. They may then use their control of multiple accounts to play both sides of the conversation in an email chain to make the attempt seem legitimate.

It is often difficult to identify exactly when an IT system compromise occurred, but good cyber security and user awareness, knowledge and discipline helps to prevent attempts from being successful.



Remember

- Don’t click on unsolicited links in emails.
- Don’t open unknown attachments.
- Have a unique and complex password for your NHS.net (or equivalent) email account.
- Report anything suspicious immediately to your manager and/or IT team.
- Ensure your IT team carry out system updates to ensure the latest patches and firewall updates are installed promptly.

Red flags for mandate fraud

What is the sender's email address?

Get into the habit of holding your mouse over the sender's email name. This exposes the actual email address behind the name that appears. It is easy to change the sender's name to appear as whatever you want it to be, as it does not have to be the actual email address. If you hover over the name, you will be able to see the real email address and can cross reference this against your previous correspondence and records.

Attempts are often made from email accounts which are designed to look similar to that of a genuine supplier. In links to the NHS email domain (@nhs.net), we have seen fraudsters replace the "**n**" with an "**r**". In other examples, we have seen fraudsters often replace an "**m**" with an "**rn**" and replace a "**d**" with a "**cl**". Usually, it is a small change that's made, which might not be immediately obvious, but that small change is enough to ensure correspondence is controlled by a fraudster.

Is there a sense of urgency?

Fraudsters are most successful when they can instil a sense of panic into the victim. Often payments are made in a rush before the sender has a chance to stop and think, and therefore realise something is amiss. Mandate fraud emails often create a sense of urgency; for example "my train is delayed, and I can't access the systems, can you please send over £5,000 to Mr Morris in my absence." Remember there is always five minutes to take a moment, check with a colleague, or call the person you think has sent the email to check it did come from them. It is always better to wait and check, than act in haste and fall victim to fraud.

Are they asking you to go outside of the usual process?

It is common for fraudsters to encourage you to bypass the formal and official process. Be alert to such requests as it is unlikely that any of your colleagues will ever ask you to act outside of the usual procedures. Although sometimes these things do happen, if you are asked to act outside of usual process, contact the person you think has sent you the request using previously used contact details and check with them before acting. Do not be afraid to query more senior staff. The Chief Executive will be happy to provide authorisation if it is a genuine request.

Are there grammar and spelling mistakes?

When fraudsters make attempts to commit mandate fraud, they may be from overseas, with English not being their first language, or they are making attempts in such a hurry, that they make grammar and spelling mistakes. Often, the first sign of something suspicious, is the misspelling of words or emails that don't read well. Additionally, if you know the person that the email is purporting to be from, you are likely to be familiar with how they usually communicate, and this will be a further indicator.

What to do if you spot a possible mandate fraud attempt

1. Check the contact details

Verify the request by making direct contact with someone you have dealt with previously to check the request is legitimate. Always use known communication channels held in pre-existing records and never use the phone numbers or email addresses supplied on the request you have received. Use known details to check the responses you receive or cross-reference them to a genuine website. You could also consider asking your contact to verify information from previous correspondence or invoices that would only be known to them.

2. Stop the payment

If you think a payment has been made to a fraudulent account, contact your bank immediately. Payments are normally made using the standard BACS process and take three working days to arrive in the beneficiary account. The payment can often be reversed if caught early enough. A CHAPS or Faster Payments will transfer more quickly, but if notified promptly, the bank may be able to freeze the beneficiary account if it is held by them or contact the onward bank to attempt to freeze the account while enquiries are made. This will also add a fraud flag that may prevent others from becoming victims.

3. Tell someone

If you suspect a fraudulent payment has been made, or a fraudulent request has been received this should be flagged immediately to your supervisor. Fraudsters often target several people at once, so although you may have identified the request as fraud, a colleague may be about to make or authorise the payment. Your IT department can look to secure any compromised email accounts and block fraudulent email domains and IP addresses, preventing future attempts.

4. Freeze the supplier account

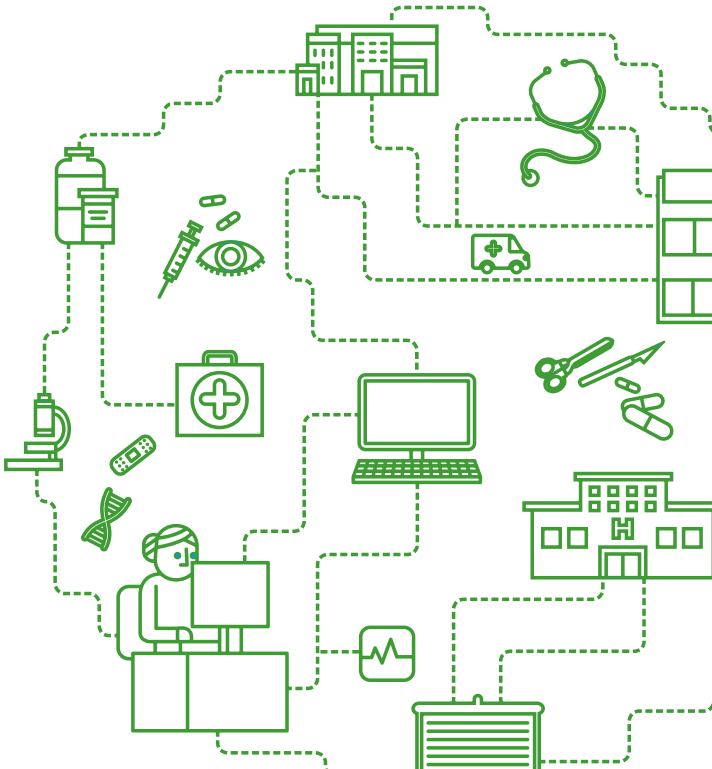
The supplier account should be frozen to prevent any changes being made or payments sent. This allows a further investigation to commence without there being a risk of others sending money.

5. Do not engage

You should not seek to lure the fraudster to provide more details or engage with them further. When they elicit a response, they may be more inclined to keep trying and further target your organisation. If controls are strong and no payment is made, they will move their focus to another organisation where they have more chance of success.

6. Report the attempt

All attempts of fraud against the NHS must be reported to your LCFS or directly to the NHSCFA. Contact your LCFS as soon as you suspect a mandate fraud attempt has been received. You should retain all communication as this may be needed as evidence. We will liaise with your IT department to ensure any electronic evidence is secured.



For further information contact

Matt Wilson

Associate Director

LCFS

07484 040 691
matt.wilson@rsmuk.com

Kirsty Clarke

Assistant Manager

Lead LCFS

020 3201 8054
kirsty.clarke@rsmuk.com

You can also report concerns of suspected fraud to the NHS Counter Fraud Authority on 0800 028 4060 or through their reporting form https://cfa.nhs.uk/reportfraud.