NHS
Counter Fraud Authority

Mandate Fraud Supplier Guide

October 2022 | Version 1.0

The purpose of this guidance is to highlight the risks of mandate fraud to NHS suppliers.

Who is this guidance for?

Companies supplying the NHS.

The NHS expects suppliers to be vigilant and proactively look for fraud, including the risk of fraud in their own business dealings with the NHS.

What is mandate fraud?

Cyber-enabled crimes are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of Information and Communications Technology (ICT) (such as cyber-enabled fraud and data theft). Mandate fraud is one such type of cyber-enabled fraud.

Mandate fraud, also known as Payment Diversion Fraud, can be defined as a request to change banking information (direct debit, standing order, bank transfer mandate) submitted typically via email by an individual or group purporting to be a genuine business, such as a supplier to the NHS.

False or spoofed email addresses are often created to appear like the genuine business. Fraudsters have acquired domain names that are very similar to suppliers' genuine domains or the NHS or have used software to mask their address and make it appear emails have come from suppliers. They then submit false invoices, or request a change in bank/mandate details, appearing to be communicating from the legitimate supplier.

Social engineering is a significant part of the cyber enabled mandate fraud process where cyber criminals 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 due to 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.

Please see the 'Guide to cyber attacks' for further information, which sets out 13 different techniques used by cyber criminals.

Types of 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 a supplier's bank account details.
- An email request is received from an email account purporting to be from an NHS finance staff or another supplier.
- 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 sent from a genuine supplier email account, where the account has been hacked and taken over, and request made to divert outstanding and future invoices to a new account number.
- An email is received from an email address, which is very similar to the genuine one, with a minor amendment to the sender's address details. For example, the genuine address is Joebloggs@nhs.net but the fraudulent email came from Joebloggs@nhss.net. Always check the authenticity of an email received (e.g. the domain name) by using established contact details already held on file.
- A written request is received in the form of a letter or invoice that is either forged (amended from a genuine version), or counterfeit (made to look like a genuine version), but is not sent from the supplier or the NHS.

How to protect yourself

Cyber Security

Cyber security is the means by which individuals and organisations reduce the risk of being affected by cyber-crime. It is important to stay safe online to prevent cyber criminals getting hold of our accounts, data, and devices.

- Review cyber security processes and procedures
- Ensure employees are trained to recognise fraud and cyber attacks
- Update your devices with the latest software and anti-virus updates
- Back up your data.

Passwords

Passwords remain the default method of authentication for a huge range of services, both at work and at home. The increase in password use is mostly due to the surge of online services, including those provided by government and the wider public sector, and the massive growth in use of personal computers, smartphones, and tablets.

According to the National Cyber Security Centre, simply typing in the word ‘password’ allowed fraudsters to gain access to 3.6million accounts worldwide and a staggering 23.2 million accounts used ‘123456’ as a password. Another 3.8 million accounts were hacked using “qwerty” - the first six letters on the top left of a standard keyboard. Using favourite names, football teams, bands and fictional characters also exposed millions to hacking.

Cyber criminals can get access to your account by using software to guess your password or by trying to trick you into disclosing your password through scams. Creating strong, separate passwords and storing them safely is a good way to protect yourself online.

- Promote strong password management procedures
- Use a strong and separate password for your email
- Create strong passwords using 3 random words, with embedded capitals, numbers and special characters
- Save your passwords in your browser
- Turn on two-factor authentication (2FA)
- Set a limit of the number of failed attempts before an account is locked

Other

- Do not give out bank details over the phone.
- Staff should regularly review the Outlook Rules on their email accounts to see if their emails are being diverted.
- Where, in the event that, contact is made regarding NHS payments for your services, contact the NHS Trust finance team using the details you have on your system.
- NHS Finance Teams seek to verify all changes to supplier details they receive. Be aware that they may not pay invoices until they have fully verified changes. Please ensure you are able to respond to them promptly.

What to do if you suspect mandate fraud?

- Contact the NHS Trust finance team immediately using a known contact and contact details.
- Contact your bank immediately and ask them to reverse or freeze any payments made.

Why take action?

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

Other Guidance

- Suppliers code of practice: preventing fraud, bribery and corruption (cfa.nhs.uk)

Resources

- For a guide to Cyber threats, see the following: Cyber Threats (cfa.nhs.uk)
- Test your knowledge on cyber fraud: Cyber Quiz (cfa.nhs.uk)
- Using passwords to protect your data- NSCS
- Avoiding phishing attacks - NCSC
- Fraud | NatWest Business