FPN: Mandate Fraud – requests to change phone numbers

Published by Andrew Masterman on 29 March 2021 12:34

Priority action	High	X	Moderate		Low	

Unique Reference Number	H-002-21
Date issued	29 March 2021
Subject	Mandate Fraud – requests to change phone numbers
Distribution list	Directors of Finance (DOF's) Chief Financial Officers (CFOs) Local Counter Fraud Specialists (LCFSs) Audit Committee Chairs (ACCs)
Relevant documents	• Invoice and Mandate Fraud quick guides • Mandate fraud circular G/08/2018-19 • CEO email fraud circular CG/09/2018-19 • FPN H-001-19 – Bank Mandate Fraud – payroll changes • FPN H-010-20 Mandate Fraud

Background

In March 2021, the NHSCFA was alerted to a mandate fraud attempt, which was referred to the NHSCFA by the Department of Health and Social Care Anti-Fraud Unit (DHSCAFU) and forms a live investigation. In this instance, fraudsters are contacting NHS organisations posing as an existing supplier and requesting a change to the genuine supplier's phone number. This is done ahead of requesting a further change to their bank mandate. This is being done by fraudsters to establish early contact prior to making a bank mandate change request and if successful to get through the NHS organisation's call back checks when bank change requests are made. In this instance, when the NHS organisation calls back to verify the change in bank details they are speaking to the fraudsters.

NHS organisations need to remain vigilant to any supplier change request of this nature and ensure they are following internal policies and procedures.

How the fraud operates

What is Mandate Fraud?

Mandate fraud is also known as payment diversion fraud, a change of bank account scam, or supplier account takeover 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.

How can this type of mandate fraud occur?

- An initial contact is made by the fraudster via telephone, email or by letter to the NHS organisation purporting to be from an existing supplier with instructions to change phone details, followed by bank account details of the supplier.
- By using early engagement, the perpetrator will request that the phone number of a genuine NHS supplier is changed.
- The perpetrator will then make a follow up request that bank mandate details are changed and transferred, usually as a matter of urgency, into an alternative bank account.
- The staff member receiving the request may feel pressured to comply as instructed due to the urgent nature of the request of changes to be made. In this instance, where a fraudster had successfully requested a change to a phone number, when the staff member makes the call back process, they are actually speaking to the fraudster, rather than the genuine supplier.
- The fraudster may use 'socially engineered'[1] information from the NHS organisation to appear genuine and gain the trust of the NHS organisation staff member, such as appearing to be the genuine person they are purporting to be, having an understanding of internal systems, to gain the trust of the staff member and persuading them to act in such a way as to make the fraud more likely to succeed.

Prevention advice

To protect against this type of fraud, please consider the following:

- Raise awareness and ask staff to be vigilant of this new *Modus Operandi* to bank mandate fraud where fraudsters request that a supplier's phone number is changed ahead of requesting bank mandate changes.
- Staff should check the details of the person making the request and the supplier's details, before responding on each and every occasion.
- Any requests for changes to a supplier's phone number must go through an NHS organisation's own independent verification process. This will include

contacting the supplier by using the details held on the NHS organisation's system, prior to making any changes. This verification process should include conducting checks against pre-existing records on the person making the request and on the company details.
- Staff members must escalate *all* suspicious requests to their line managers as soon as possible, in accordance with the organisation's fraud reporting route and policy so that any immediate action can be taken.
- Any requests to change a bank mandate should follow the NHS organisation's procedures, see Further Information below.
- Regular checks should be undertaken on bank statements to look for any suspicious activity.
- Ensure that all staff (at least) undertakes fraud awareness training annually.
- Procedures should be amended if necessary, to reflect these mitigation measures and staff should be made aware of the amendments.

Action to take

- Raise awareness of this type of fraud by disseminating the information in this alert to all finance teams and put in place the measures given above.
- All incidents of suspected fraud against the NHS organisation should be reported to the nominated LCFS and the NHSCFA (by calling 0800 028 4060 or online at www.cfa.nhs.uk/reportfraud).

Further Information:

- See also Circular G/08/2018-19, 19/12/18: 'Mandate fraud: key risks and fraud prevention recommendations (following recent fraudulent attempts at NHS health bodies)'
- Circular G/09/2018-19 'CEO email fraud: key risks and fraud prevention recommendations (following recent fraudulent attempts at NHS health bodies)'
- FPN H-001-19 – Bank Mandate Fraud – payroll changes
- FPN H-010-20 – Mandate Fraud.

Handling information

This document may be circulated in accordance to the agreed distribution list below.

No recipient is permitted to share this document outside of their department or agency, without prior permission from the author. Any further dissemination requests or feedback on this document should be directed to prevention@nhscfa.gov.uk.

Internal	
Team/Individual Name	Handling Instructions
NHSCFA internal Business Units	[Official]

External	
Organisation/Agency/Team/Individual	Handling Instructions
All LCFS and DoFs Finance Teams HR/Payroll Teams	[Official]

Contact details

Fraud Prevention Team
NHS Counter Fraud Authority
80 London Road
London
SE1 6LH

Email: prevention@nhscfa.gov.uk

Text for dissemination

The information contained in this FPN is classified as Official and should only be shared with those staff identified above in the Handling information.

---

[1] Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses manipulation to trick users into making security mistakes or giving away sensitive information.