Bank Mandate Fraud

NHS National Services Scotland

What is Bank Mandate Fraud?

This describes the fraudulent changing of bank account details for a supplier of goods or services or any other beneficiary, to divert payments from your organisation to an account controlled by the fraudster.

How does it work?

Here is an example of how the mandate fraudster operates. Walk around any town centre and you will see huge banners attached to scaffolding identifying a roofing company or building contractor doing work for a business. This provides great information for a fraudster who can use knowledge of this business relationship and the nature of the contracted work to pretend to be the roofing company. The fraudster contacts the owner of the building pretending to be the building contractor and tells them that their business bank account has changed. They request future payments be sent to a new account which is under the control of the fraudster. These accounts often belong to unwitting distant associates of the fraudster, who often targets students and more recently, children. This type of fraud has been highly successful in taking huge sums of money from public sector organisations.

Often the first alarm is raised by the contractor enquiring after a late payment but this can happen long after the monies have left the fraudulent account and moved out of the reach of both the banks and law enforcement.

What are the consequences?

Public money is lost as the genuine contractor still has to be paid. Through paying twice for goods or services, monies must be diverted from its intended purpose for the public good. This diversion can result in public services being delayed, down-scaled or cancelled and cause reputational damage to the organisation. A significant but often overlooked consequence is the impact that the fraud has on the honest employee who administered the recording of false bank details, believing them to be genuine.

Managing the risk

Carefully scrutinise all changes to bank accounts by taking the following steps:

- request the current bank account details as well as new details
- ask the supplier company to confirm the change, preferably through a known, named contact
- use your existing contact details/signatures to phone or email the supplier, not those on the change request
- line managers must rigorously check the change request documentation and the steps taken to verify the request before authorising the change of bank details
- adopt 2-factor authentication for changes, not just email
- verify callers are who they say they are - call them back via the supplier's telephone switchboard or email a known person
- check the URL for small differences in spelling and suffix domain names e.g. .co.uk instead of .com

NHSCOTLAND CFS COUNTER FRAUD SERVICES

Fraud.
Together we can stamp it out.

Bank Mandate Fraud

NHS National Services Scotland

Don't make it easy

- bank account details are acquired by individuals and data-wholesalers who trade in leaked, hacked and elicited data so read and apply your IT security and information governance policies to help protect your business data
- read your organisation's financial instructions to ensure that your processes align to all relevant requirements
- read and apply any local policy on managing supplier payments; consider reviewing and updating this or creating a 'standard operating procedure' to help identify and manage the risk
- adopt a clear desk policy and lock away documents that can be manipulated to change bank account details
- destroy supplier data when no longer required
- weed your approved supplier list to remove companies that you haven't purchased from for a lengthy period of time.

Did you know?

- fraudsters can gather our contractors' details from information which public bodies publish online or even elicit the names of our building and facilities' contractors from on-site signage
- Companies House data is only a register and details can be changed by the fraudsters
- CFS issues alerts to partner organisations providing the latest intelligence about the tactics used by bank mandate fraudsters

It's fraud-time

Fraudsters know that people are less attentive to workplace detail when their focus starts to shift towards their leisure and family time. Consequently, they often launch fraud attacks late on Friday afternoons and just prior to holiday weekends.

Fraudsters also know that we are distracted during busy periods like the financial year-end. Never be afraid to contact a supplier at any time, as they will understand the importance of verifying the accuracy of payment information.

If it happens to you

- don't delay, report it to your manager
- contact your bank immediately to see if the payment can be stopped/recalled
- advise your organisation's Fraud Liaison Officer and the CFS intelligence Team **NSS.cfsintelligence@nhs.scot** telephone **01506 705 100**

CFS will consider alerting other partner organisations to the potential threat by issuing an Intelligence Alert

If you would like a presentation about fraud risks in the finance department, contact us at nss.cfscommunications@nhs.scot

Visit our website for more information on all of our services www.cfs.scot.nhs.uk and follow us on Twitter @NHSSCFS

Fraud Hotline
08000 15 16 28
Powered by Crimestoppers
cfs.scot.nhs.uk