Dear Supplier

RE: Cyber Enabled Mandate Fraud

Mandate fraud is also known as ‘payment diversion fraud’, a ‘change of bank account scam’, or ‘supplier account takeover fraud’. Genuine supplier details are usually obtained from a range of sources including corrupt staff, publicly announced contracts and online logs of supplier contracts. The change of bank details element may be preceded by a request to change key contact / phone details.

Fraudsters are also using ‘social engineering’ techniques to facilitate this fraud, by applying pressure in different ways (i.e. the need to process account changes in order to meet an urgent payment deadline) to force changes through without the usual, cautious validations checks being carried out.

There have been several incidents of cyber enabled supplier mandate frauds in the NHS recently, both prevented and detected. Cyber criminals in these instances are using tools such as phishing emails to access the email accounts and IT systems of NHS organisations, and suppliers too, in order to obtain sensitive financial data.

Once the cyber criminals have access to email accounts, they can then intercept the communications between NHS organisations and their suppliers in relation to their business transactions and financial accounts. Genuine invoices are resubmitted by the cyber criminals, posing as the genuine supplier, with a request to change bank account details and divert the funds to a criminally controlled bank account.

It is believed that in some incidents, the cyber criminals are part of an Organised Crime Network, and the stolen monies are subsequently laundered and used in further serious criminality.

There have also been instances where fake internet / email domains have been set up to fool organisations into sharing or changing their bank accounts details.

For example, if fraudsters were masquerading as ‘Manchester City’ they could set up a fake domain of XYZ@mɑnclty.com, when the real domain is XYZ@mancity.com, and anyone glancing at the email may not see that the “i” has been replaced with an “l”.

You may not have noticed that there was another change in the fake domain above, in that the Greek letter ‘ɑ’ has been added instead of the regular, Cyrillic letter “a”.

Those with financial responsibilities at NHS organisations have recently been reminded again by the NHS Counter Fraud Authority to remain vigilant to any supplier change of bank account requests.

NHS organisations are also being urged to highlight the cyber enabled mandate fraud threat with their suppliers, hence this letter.

In order to protect the NHS and yourselves against this type of fraud, please can you:

- Raise awareness of this issue (and share this letter) with your finance team and other key personnel to ensure they are vigilant to the risks of cyber enabled mandate fraud.

- Raise any concerns you have regarding whether your own email or IT systems have been compromised.
    - With your own IT team to take appropriate action and secure vulnerable or compromised email accounts
    - With your Senior Management / Executive Team, for oversight
    - With your own clients, suppliers and partners, so that they are made aware of the situation and are vigilant to requested bank account changes made in your organisation's name
    - With Action Fraud (0300 123 2040 or online at https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime) to report any actual frauds against your organisation

- Take steps to try to close down any fake domains masquerading as your organisation's name and prevent them operating. You can also report phishing emails or fake company websites to the National Cyber Security Centre via:
  https://www.ncsc.gov.uk/section/about-this-website/report-scam-website
  https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email

- Block any fake domains from interacting with your own email / IT systems (in the example above @mɑnclty.com could be blocked as both a sender, cc, bcc and receiver of emails via your email server).

Please also be aware that NHS staff will be checking the details of the person (supplier) making the request when they receive a bank mandate change submission, utilising existing contact details. Please assist this process by responding to any such requests in a swift and timely manner.

Please can you provide a response by return e-mail to confirm that you have taken appropriate steps and actions to mitigate cyber enabled mandate fraud within your organisation.