Mandate Fraud

Mandate fraud is when someone gets you to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example a business supplier. Also known as payment diversion fraud.

Method

A form of mandate fraud, known as CEO fraud, will typically start with a "spoof" email being sent from a fraudster to a member of staff in a company's finance department, but may be sent to the procurement or other account holder. The member of staff will be told by the fraudster who is purporting to be a company director or CEO that they need to quickly transfer to a certain bank account for a specific reason. The member of staff will do as their boss has instructed, only to find that they have sent money to a fraudster's bank account.

There have been many other versions that include requesting payment details changed on existing vendors accounts. The fraudster will normally redistribute this money into other mule accounts and then close down the bank account to make it untraceable. Very little of the funds are ever recovered.

Tactical advice

- Educate staff about this type of fraud in order to prevent themselves becoming a victim.
- Ensure all staff, not just finance teams know about this fraud.
- Encourage double checking, and never be rushed into transferring large amounts, even if it is purported to be an important task given by senior managers.
- Compare email addresses and other details to previous correspondence.
- Have a system in place which allows staff to properly verify contact from their CEO, senior leadership, for example having two points of contact so that the staff can check that the instructions which they have received are legitimate.
- Always review financial transactions to check for inconsistencies/errors, such as misspelt company name.
- Changing bank accounts is an unusual occurrence; therefore always verify changes to financial arrangements with an organisation directly using established contact details you have on file.
- Do not be afraid to question when you are dealing with new accounts, or where there has been a period of time between purchase orders. If in doubt request clarification from an alternatively sourced email address/phone number.
- Do not be afraid to question when you are dealing with a vendor that you have not previously dealt with.
- Do not be afraid to question when the delivery address differs from the historical ones.
- Never leave invoices, regular payment mandates or similar information unattended for others to see.
- Consider what information is publicly available about the business and whether it needs to be public.
- Ensure computer systems are secure and that antivirus software is up to date.

To report a fraud and receive a police crime reference number, call action fraud on 0300 123 2040, or call 101.