Invoice fraud

Invoice fraud occurs when a fraudster sends you an email or letter, or calls you purporting to be from a supplier/customer, and advises of a change of bank details or provides new bank details for payment. When the invoice or payment is made it is actually to an account controlled by fraudsters.

The fraud may only be discovered when the legitimate supplier follows up on non-payments.

Fraudulent letters and emails sent to companies are often well-written, meaning the fraud is difficult to spot without strong operating processes and controls in place.

Legitimate customers/suppliers can have their email accounts hacked. Fraudsters can send emails from any email address and disguise them as being sent by a recognised sender. They can even insert fake emails into existing genuine email trails.

CEO Impersonation Fraud

A variation on invoice fraud, this is when an email purporting to come from a senior official within your organisation requests a payment with bank details provided, but which has actually come from a fraudster.

Protecting your business against invoice fraud and CEO impersonation

- Be cautious of how much information you reveal about your company and key officials via social media platforms
- Make your staff aware of this threat, particularly those that make and/or process payments
- Any payment requests with new or amended bank details received by email, letter or phone should be independently verified. This includes internal emails from senior management that contain payment requests. Ensure that you validate the exact bank detail changes you should be making in full
- Consider setting up single points of contact with the companies you pay regularly
- Regularly conduct audits on your accounts
- Electronic payments in the UK are made based on sort code and account number only, and any account name given is not routinely checked, therefore independent verification is important.

Case study

A company in the property sector was required to pay their supplier over £102,000 at the end of the month. Not long before the payment was due, they received a message advising of a change of account details. The payment was duly made to the new account as instructed. A week later, the genuine supplier called to ask why they had not received their funds.

As a week had passed, there was now only £300 left in the account used by the fraudsters – the rest had been withdrawn and spent. Consequently, the company's bank were unable to offer any assistance in recovering the funds.

"Invoice fraud can be devastating for a small business. It is important that employees are able to spot the signs of an attempt and that a strict policy is in place when making changes to payment details. This should require checking the changes with the company concerned by contacting them directly through existing contacts, as well as require a manager to check and sign off the changes."

DCI Andrew Gould
Operation Falcon, Metropolitan Police Service