

Counter Fraud Factsheet

Payment Diversion Fraud



What is it?

Payment diversion fraud happens when someone gets you to change a direct debit, standing order or bank transfer mandate, by claiming to be from an organisation or supplier you make regular payments to. Also known as mandate fraud this type of fraud is usually attempted over the phone or by email.

Case Example

A local council authority in Northern Ireland was defrauded out of £400,000 after falling victim to mandate fraud.

The scam only came to light after a contractor enquired about missing payments. Despite receiving assurances that the money had been paid, it failed to appear in their bank account.

A subsequent investigation found the account details of the legitimate firm had been accessed by someone posing as a council representative.

Another person acting as the contractor approached the council for payment and provided new bank details. The funds were then transferred to the bogus account.

How to prevent this type of fraud

Changing bank accounts is an unusual occurrence, therefore:

- The supplier's contact details should be taken from existing records held by the health body and not from information supplied in the change request.
- Staff should check the authenticity of an email received from a supplier (e.g, the domain name) by using established supplier contact details already held on file.
- If a call from an alleged supplier seems suspicious, hang up and call the organisation using established contact details.
- Always review financial transactions to check for inconsistencies/errors, such as misspelt company names, chief executives or financial directors.
- Organisations should ensure relevant policies and procedures are communicated to all staff involved in the payment process.