

THE CHECK BEFORE YOU PAY

Practice money, paid to the real supplier.

A practice pays suppliers, locums and staff with a small team and often no IT department of its own, which is exactly the gap a payment diversion email is written for.

How it happens here

1. Regular payments found

Fraudsters find out which suppliers the practice pays regularly.

2. A busy time chosen

They often time the request for a busy period in the practice.

PRESS CHECK HERE

3. New details arrive

An email in the supplier's name says its bank details have changed.

4. The money goes

Unless somebody rings the supplier on the number already on record, the next payment goes to the fraudster.

Before any payment to new or changed bank details

- 1 Never change a supplier's, locum's or employee's bank details because of an email alone.
- 2 Ring them on the number already on your records, not one in the email, and check that number was not itself changed recently.
- 3 Check every invoice against something the practice actually ordered and received.
- 4 The practice manager or a partner, not the person who took the request, approves the change.
- 5 Run Confirmation of Payee, and for a new account send a small amount and have the payee confirm by phone.

If money has gone

Ring your bank's fraud line at once, then report to Report Fraud on 0300 123 2040 or reportfraud.police.uk (Police Scotland on 101 in Scotland).

Also on day one for NHS-funded work: report to your Local Counter Fraud Specialist or the NHS Counter Fraud Authority.

What your sector's own bodies say

- Verify a change of supplier details using contact details already on file, and check those were not themselves changed recently; use Confirmation of Payee and question any mismatch; separate duties; freeze the payment and report as soon as something looks wrong. (NHS Counter Fraud Authority, Payment diversion fraud guidance, version 3.0, July 2026)

Where Jatzo fits. Jatzo does not replace the call. It helps whoever reads the email notice that it needs one, before anybody pays.

Check before the supplier is paid

Anybody unsure about a supplier's new bank details, or an invoice nobody remembers ordering, presses Check in Outlook or Gmail for a score out of 100 with the reasons.

Your practice manager hears at once

When anybody checks a message scoring High risk or above, an email goes to addresses you choose at your own domain, such as your practice manager's.

More at jatzo.co.uk/for-teams/healthcare

Each invoice against confirmed details

Invoice Fraud Analyser, a separate Windows program, compares the bank details on each supplier invoice with the ones you confirmed, and says Stop when they differ.

Training for reception and admin

Business Pro includes every Training Centre course for everyone in the team, Invoice and payment fraud among them, with a record of who completed it.

UK Finance recorded £41.3 million lost to invoice and mandate fraud across 2,305 cases in 2025, 68% of it from business accounts. Criminals intercept emails or take over an email account, then pose as a supplier, a solicitor or a builder with new bank details. (UK Finance, Annual Fraud Report 2026, June 2026.) Report Fraud replaced Action Fraud in December 2025; the number did not change.