

THE CHECK BEFORE YOU PAY

Client money, paid to the client.

A practice moves other people's money every day: tax refunds, payroll and supplier invoices. That makes an email with new bank details look routine, which is exactly why it works.

How it happens here

1. Money is due

The practice is about to pay a client's tax refund, or run a client's payroll.

PRESS CHECK HERE**2. New details arrive**

An email in the client's or an employee's name gives new bank details for the money.

3. It looks routine

A practice moves other people's money every day, so new bank details look like routine work.

4. The refund goes elsewhere

Unless somebody rings the client on the number on file, the money goes to an account the client never gave.

Before any payment to new or changed bank details

- 1 Never change a client's, employee's or supplier's bank details on the strength of an email alone.
- 2 Ring the person on the number already on your file, not one in the email, and note the call.
- 3 Before any refund or client money leaves client account, confirm the destination account by phone.
- 4 A second person approves every bank detail change and every client money payment.
- 5 For a new account, send a small amount first and have the payee confirm receipt 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: tell the client, notify your professional indemnity insurer, and consider a Suspicious Activity Report to the National Crime Agency.

What your sector's own bodies say

- Treat unexplained bank detail changes as a red flag, verify them against details already on file through contacts you already trust, and split supplier set-up, approval and payment between different people. (ICAEW, How to identify and deal with fake invoices, February 2026)
- After a diverted client refund, tell the client, notify your professional indemnity insurer promptly and consider a Suspicious Activity Report. (ICAEW, Fraud issues for members in practice, updated January 2025)

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 refund goes

Anybody unsure about a client's new bank details presses Check in Outlook or Gmail and sees 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/accountants

Every invoice against confirmed details

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

See what is aimed at the practice

The organisation threat report counts the checks that reached Suspicious or above by kind of attack, the last 30 days against the 30 before, and names nobody.

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.