

THE CHECK BEFORE YOU PAY

Stage payments, paid to the real supplier.

Long supply chains, frequent high-value payments and payment instructions sent by email are why the National Crime Agency singles out construction for invoice fraud.

How it happens here

1. Emails intercepted

Criminals intercept a supplier's emails, or impersonate the supplier, and learn who is due to be paid.

2. A valuation is agreed

A stage of the work is valued and a large payment to the subcontractor or supplier falls due.

PRESS CHECK HERE**3. New details arrive**

A convincing email or invoice says the bank details have changed, with pressure to pay quickly.

4. The stage payment goes

Unless somebody rings the supplier on a number used before, the payment goes to the criminal.

Before any payment to new or changed bank details

- 1 Never change a subcontractor's or supplier's bank details because of an email or letter alone.
- 2 Ring them on a number you have used before, not one on the invoice or the email.
- 3 Check the invoice matches the order, the valuation and the work done before it is approved.
- 4 A second person, not the one who received the request, approves the change.
- 5 For a first payment to new details, send a small amount and have the supplier 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).

What your sector's own bodies say

- Check for changes to invoice or bank details, be wary of pressure to pay urgently, and verify by calling the genuine supplier on a number you have used before. Never transfer money until you are satisfied the details are correct. (National Crime Agency and National Federation of Builders, March 2026)

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

Every invoice against confirmed bank details

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

Your finance lead 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 finance lead's.

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

Check before the stage payment

Anybody in the office unsure about a supplier's new bank details presses Check in Outlook or Gmail and sees a score out of 100 with the reasons.

Training for site and office alike

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.

Report Fraud's analysis for 2024/25 found construction and manufacturing were the two sectors most affected by invoice fraud. (National Crime Agency and National Federation of Builders, March 2026.)

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.