

THE CHECK BEFORE YOU PAY

Supplier invoices, paid to the real supplier.

A business that buys materials, stock or freight from a long list of suppliers pays large invoices every week, and most of the paperwork arrives by email. The National Crime Agency puts manufacturing beside construction as the sectors invoice fraud hits hardest.

How it happens here

1. Invoices every week

Materials, stock and freight are paid for every week, and most invoices arrive by email.

2. A mailbox is hacked

Fraudsters hack a supplier's or haulier's email account, or register a domain that looks like it.

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

An invoice from a contact you deal with every week gives updated bank details.

4. The invoice is paid

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

Before any payment to new or changed bank details

- 1 Never change a supplier's, haulier's or customer'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 in the email.
- 3 Match every invoice to a purchase order and a delivery before it is approved for payment.
- 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, invoice fraud campaign, March 2026)
- It is rare for a business to change bank accounts, so treat any request to do so with caution, confirm the old and new details on a known phone number, and consider waiting 14 or 30 days before new supplier details are approved. (GOV.UK, Stop! Think Fraud: Protect your business, current guidance)

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

Each supplier invoice, checked before payment

Invoice Fraud Analyser, a separate Windows program, compares the bank details on every supplier and haulier 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/manufacturing

Check the email that changes details

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

See what is aimed at the business

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.

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.