

THE CHECK BEFORE YOU PAY

Completion money, sent where it should go.

Conveyancing is where an email that changes bank details does the most damage: a deposit, a completion or sale proceeds sent to a criminal's account, often late on a Friday. This is the check that stops it, and where Jatzo fits.

How it happens here

1. The chain is read

A criminal reads the email chain on a matter, or forges one, and waits.

2. Completion draws near

They act close to exchange or completion, when money is about to move and everybody is busy.

PRESS CHECK HERE

3. New details arrive

An email in the seller's name gives a new account for the proceeds, often on a Friday afternoon.

4. The money goes

Unless somebody rings the client on the number from the start of the matter, the money goes to the criminal.

Before any payment to new or changed bank details

- 1 Never act on bank details that arrive or change by email alone, whoever appears to send them.
- 2 Ring the client or the other firm on the number on the file from the start of the matter, never a number in the email.
- 3 Check new details against documents already on file, and record the call on the file.
- 4 A second person, not the fee earner who received the email, approves any change before money moves.
- 5 For sale proceeds, send £1 first and wait for the client to confirm by phone that it arrived.

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: replace the client money as the SRA Accounts Rules require, report to the SRA, and tell your indemnity insurer.

What your sector's own bodies say

- Treat a late request to change bank details as a possible cyber attack, ring the client on the number recorded at the start of the matter, and consider a £1 test payment, confirmed by the client, before the balance. (Law Society, Practice Advice Service FAQ: cybersecurity, August 2026)
- Report cyber attacks that stop transactions or put client money at risk to the SRA promptly; serious breaches must be reported under the Code of Conduct for Firms. (SRA Update 123: cybercrime, January 2024)
- The SRA publishes scam alerts naming domains set up to impersonate real firms. (SRA scam alert, August 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 proceeds go

A fee earner unsure about an email presses Check in Outlook or Gmail and gets a score out of 100, with the reasons, before anybody pays.

Web addresses that copy your firm's

Domain Watch looks for new web addresses made to look like your firm's, the trick the SRA's scam alerts describe, and checks whether anybody can send email as you.

More at jatzo.co.uk/for-teams/law-firms

Your COLP hears at once

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

A record for your indemnity insurer

Business Pro builds a dated proof pack of the checks your firm made, the training completed and the domains you watch, for an insurer's or client's questionnaire.

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.