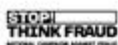




New Scam Alert: Protect yourself from payment diversion fraud when buying a new property.

City of London Police and Action Fraud, the national reporting centre for fraud and cyber crime, are urging the public to remain vigilant following a rise in payment diversion fraud - commonly known as conveyancing fraud. This type of fraud often involves criminals impersonating solicitors or estate agents to intercept large financial transfers during property transactions.

Between 1 April 2024 and 31 March 2025, 143 cases of conveyancing fraud were reported to Action Fraud, resulting in £11.7 million in losses. The vast majority involved residential property transactions, accounting for 140 reports and £10.97 million in losses, with an average loss of £78,393 per case.



What is conveyancing fraud or payment diversion fraud?

Conveyancing fraud, also referred to as lawyer or solicitor impersonation fraud, occurs when criminals gain access to email chains between property buyers, sellers, solicitors, and estate agents. Once inside, they impersonate a trusted party and send convincing messages requesting that funds, such as deposits or final payments, be transferred to bank accounts

under their control.

These scams are often timed to coincide with the final stages of a transaction, when large sums are expected to be moved quickly. Fraudsters apply pressure, claiming urgency, and convincing victims that delays could jeopardise the deal.

This type of fraud isn't limited to home purchases - it has also been reported in rental agreements and probate transactions, where funds are transferred as part of estate settlements. Fraudsters will often use hacked or spoofed email accounts so that their messages can appear highly authentic. Victims may not realise they've been deceived until the money is gone.

How to protect yourself from conveyancing fraud:

- **Receiving bank details securely:** always get your solicitor's bank details in-person or over the phone at the start of the conveyancing process, and request that any changes to these details be communicated with you in-person, by phone call, or by letter.
- **Email or texts asking you to change bank details:** if you receive a message that feels suspicious, such as a request from your solicitor asking you to amend payment information, STOP! Think fraud. Contact your solicitor directly, over the phone or in-person, and verify that the request was genuine.
- **Prioritise your email security:** you should use three random words to create a strong and separate password for your email account. [Enable two-step verification](#) to add an extra level of security.

What to do if you are a victim of conveyancing fraud:

- **If you have made a payment:** inform your bank as soon as possible, they can help you prevent any further losses.
- **Report:** if you become the victim of conveyancing fraud, call your bank immediately using the number on the back of your bank card and report it to Action Fraud online at <http://actionfraud.police.uk> or by calling 0300 123 2040. If you're in Scotland, you can report it to Police Scotland on 101.
- **You could be targeted again:** fraudsters sometimes re-establish contact with previous victims claiming that they can help them recover lost money, this is just a secondary scam. Hang up on any callers that claim they can get your money back for you.

Do you want to learn more about payment diversion fraud? Check out the [City of London press release here](#).

Did you find the information in the email alert useful? Don't forget to give us a thumbs up below.