NCA
National Crime Agency

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Payment diversion fraud: conveyancing

Criminals are actively targeting property purchases, with the aim of tricking you into transferring them your house deposit and/or the balance of purchase monies to them.

These schemes can be highly sophisticated, and almost always involve the criminals pretending to be your lawyer in order to con you into diverting your payment to an account they control.

Be extremely vigilant if there appears to be any change of payment details, and always double-check by calling your lawyer before you transfer your money, as emails can be intercepted or diverted.

You can test the account by sending a small sum to the account details provided and check that your lawyer has received this before transferring all of the money.

Victims can lose hundreds of thousands of pounds, and may never get their money back.

Case study : victim of conveyancing fraud loses £640,000

A house-buyer was scammed into handing over £640,000 as part of a conveyancing fraud. Emails between the buyer and their solicitor had been intercepted by criminals. As a result, the criminals were able to collect all of the information relating to the house purchase.

The criminals then used a spoofed email account (made to look like that of the solicitor) to request payment. Payment details were provided on headed solicitors paper via the spoofed email, and the amount requested was exactly what the house-buyer had expected to pay.

The victim was later advised by the genuine solicitor that these payments had not been requested. The majority of the money was never recovered, all-but wiping out the victim's equity and savings, and leading to the collapse of their purchase. The fraud had a devastating life-long impact on the house-buyer and their personal finances.

How to protect yourself from becoming a victim of conveyancing fraud

- **Get bank details from your law firm either in person or over the phone** at the start of the conveyancing process and agree a robust mechanism by which any legitimate changes in bank details would occur, such as confirming them in person. Ask them to confirm the details by post if you've obtained them in person or over the phone.

- **Law firms rarely change their bank details. If you receive an email or telephone call stating a change in the bank details, question its authenticity**. **Always check**

the bank details directly with YOUR lawyer or someone senior at the firm by calling them on their published telephone number. Do not feel pressured into changing any details before you have spoken to someone from the firm. Check the email address carefully and if in doubt **use a trusted phone number to check the information is correct**, not the one given in the email demanding payment.

- **Set strong and separate passwords** for your accounts, and make sure that you have anti-virus software installed on your devices; these frauds usually rely on email accounts being compromised. To create a strong password, simply choose three random words. Numbers and symbols can still be added if required.
- **Avoid posting on social media about buying/selling** your house or getting a mortgage. Fraudsters may get hold of this information and, knowing the next step is a large financial transaction, seek to target you.
- **Avoid using public or unprotected Wi-Fi systems** to check emails when you are buying a house. Fraudsters can easily hack into vulnerable Wi-Fi systems.
- If you are making a payment to an account for the first time, **transfer a small sum first** and then check with the law firm using known contact details that the payment has been received.[1]
- **If you have any doubt about the transaction then do not transfer your money** until you are satisfied it is correct; **can you afford to lose your entire deposit or the entire purchase money?**

If you suspect you have been the victim of conveyancing fraud you should immediately:

- **Contact your bank** to advise them of the fraudulent activity, asking them to contact the receiving bank to freeze the funds
- **Alert your lawyer;** it may be that they are being targeted by criminals, who may pose a risk to other customers.
- **Contact Action Fraud;** report suspected fraud to **Action Fraud** through their website:www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or by calling 0300 123 2040.

NECC
NATIONAL ECONOMIC CRIME CENTRE

The Law Society

[1] Fraud - The Facts 2021 The Definitive Overview of Payment Industry Fraud, UK Finance