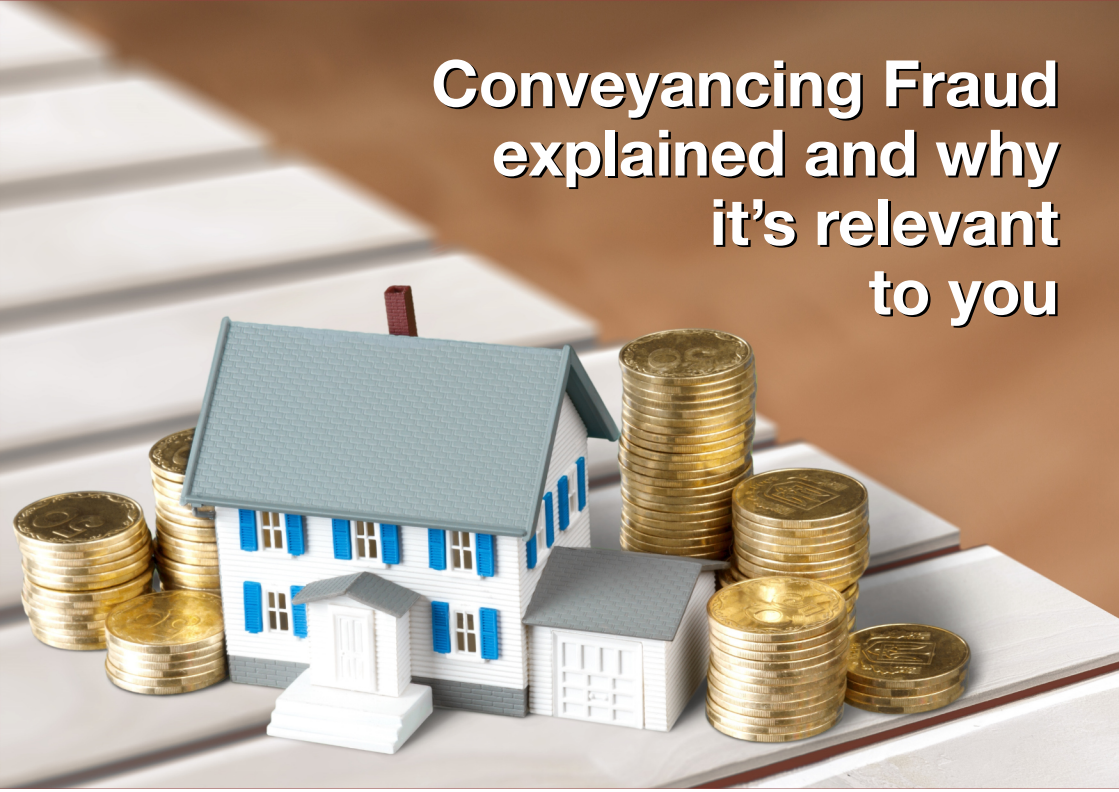
Conveyancing Fraud explained and why it's relevant to you



Conveyancing fraud occurs when the fraudster intercepts correspondence relating to the sale of a property and instructs the client to pay the funds into a new bank account that is controlled by the fraudster.

This type of crime is also known as Mandate Fraud or Invoice Fraud.

Conveyancing fraud normally occurs due to Business Email Compromise.

Once an email account is compromised, the criminal is in control of the email account and they can edit emails to suit their purposes.

Your clients need to be aware of this fraud and you need to tell them that account numbers and sort codes will not be changed during the conveyancing process.

Protect yourself, protect your clients.

Heddlu Police
DYFED-POWYS

How widespread is Conveyancing Fraud?

Dyfed Powys Police have dealt with many cases of this type of fraud and criminals are getting better at carrying it out.

Between January 2020 and December 2020 in the UK, the average loss reported by the victim was £121,586.

As people emerge from lockdown, there has been a huge increase in people looking to buy and sell houses and this provides a lucrative opportunity for criminals looking to deprive people of their life savings.

- The fraudster purports to be the conveyancing solicitor or estate agent and requests the purchasing client to transfer funds to an account controlled by them.
- Email spoofing and email hacking are cyber enabled techniques employed within conveyancing fraud and both methods are often combined.
- Funds are usually paid through a bank transfer.
- The highest proportion of conveyance frauds happen on Thursdays and Fridays.
- The primary transaction targeted was the instruction to transfer funds from the buyer to the conveyancer.
- The highest proportion of organisations that reported being a victim of conveyancing fraud were small businesses that had between 1 to 9 employees.
- Over a half of the organisations that reported conveyancing fraud have a financial turnover of less than £1.5 million.
- The financial impact on a victim of a single conveyancing fraud is significant and can have lasting effects on their financial wellbeing.
- Life savings are often lost in a single fraudulent transaction.
- The most common victims are males and females from the age range 30-39.
- Instances of conveyancing fraud are on the increase.

Heddlu Police
DYFED-POWYS

As a legal professional, what can I do?

- Tell your client – make sure they are aware of what Conveyancing Fraud is.
- Ensure your client is aware that you will never send them a change of bank account details and if they do receive such information, to contact you on a known, agreed telephone number to discuss.
- Tell the client to double check the spelling of the account, account number and sort codes are always the same as on your official literature. (Amazon is not the same as Amaz0n or Amazom)
- Print warnings advising clients that Bank Account numbers will not be changed. Put it on the front cover of your literature and make sure all old literature is either updated or destroyed.
- Ensure all emails contain reminders about Conveyancing Fraud, so the client is constantly reminded to be on their guard against it.
- Impress upon the client that they should always check with your office before making payments - on a trusted number.
- Make sure all personnel in your office are fully up to date with the latest frauds and can educate your clients about how this fraud works.
- In situations such as property purchases, the heart often takes over the head and deadlines and rushed decisions can be part of the criminals' arsenal. By placing a client under time restrictions and forcing them into a rushed decision, criminals can confuse and fool them into believing that the requests are genuine.

Business Email Compromise is the main way that these scams occur.

Criminals manage to infiltrate an email system (poor password management, insider threat or hacked database with passwords listed on them)

Once the criminal is in the email system, criminals can purport to be the genuine user.

'Rules' or 'Filters' are placed on the email systems to allow criminals to 'park' emails inside other folders, ready for them to read, and ensuring the genuine parties will not see them in the inbox.

By utilising control of the email system, criminals can change specific particulars, with the rest of the email retaining its genuine appearance – just the Payee, Account number and Sort code need to be changed.

Criminals often set up web sites and bank accounts with a similar name to the legitimate company's bank account, so the client will not recognise the slight difference in spelling.

As a legal representative, ask yourself these questions:

- Training / Awareness – are your staff fully aware about this type of crime?
- Are all of your passwords unique and strong?
- Have you checked your email system rules and filters recently?
- Do you proactively inform your clients of this type of crime?
- What steps have you taken to ensure your email system is not compromised?
- Are any other websites purporting to be you?
- What is the password policy within your organisation?
- Is all of your software genuine?
- Do you know you can forward suspicious emails to **report@phishing.gov.uk**?
- Do you know you can forward suspicious scam texts to **7726**?
- Do your staff know how to check the real sender of an email address?
- GDPR – are you aware of your obligations if your company leaks data?

Heddlu Police
DYFED-POWYS

Conveyancing fraud - Protect yourself, protect your clients.