progeny
corporate law

Cyber Crime – Fraudsters are actively targeting solicitors' clients

Clients of various firms of solicitors have been tricked by criminals into handing over significant sums of money. Further information about this type of fraud can be found on the Solicitors Regulation Authority (SRA) website at http://www.sra.org.uk/consumers/problems/fraud-dishonesty/scams.page (the SRA is the regulatory body for solicitors' practices in England and Wales).

One of the most common types of fraud is where the criminal 'clones' the identity of a firm of solicitors and sends you an email which looks like it has been sent from your solicitor. These types of emails can be very convincing and for the most part you will not be able to tell whether the email is bogus – one of the ways you can tell is if there is a slight difference in the email address used against the email addresses used by genuine employees at the firm. In these emails the payment of fees or other monies is requested and bank account details are provided for you to send the money to are provided and you are asked to make a direct transfer into a bogus bank account operated by the fraudsters. Fraudsters are able to do this because email is not a secure form of correspondence and can be accessed and altered. You can ask us not to correspond with you by email at all if you wish.

Another common type of scam is where your email address is cloned or intercepted and an email is sent to your solicitor appearing to be from you and asking for monies that belong to you to be paid from your solicitor to the fraudster's bank account. Due to this risk we will never accept instructions to send money to you by email alone. We will always verify these instructions with you by telephone or face-to-face. Until we have verified your identity and bank details to our satisfaction we will not release any monies to you. It is therefore important that you return our telephone calls or respond to our letters promptly. If you do not, then there may be delays in you receiving any monies which we hold on your behalf. In certain circumstances we may decide that the safest way to pay the monies we hold on your behalf will be by cheque.

The clients of this firm have never been targeted in these kinds of scam, but it is important that you are alert to the possibility that you could be targeted. We run strict information security, data protection and client confidentiality procedures, but it is important that you remain alert to the risks also.

In particular, please note that we will never ask you to make a payment directly to our bank account by email. Any such email you may receive will not have come from this firm and should be reported to the police and to us immediately.

If you are in any doubt about any email you receive from us you must check the authenticity of the email by contacting us directly by trustworthy means, such as by telephoning the number on our website. You must not use the number on any suspicious email you may receive as this may also be bogus and operated by the fraudsters.

If you do not follow the advice above you could stand to lose significant sums of money to fraudsters and this firm will not be liable to you for any losses unless they have occurred as a result of our negligence.

If you have any questions about the content of this note, please discuss these with us immediately.