Don’t call me, I’ll call you - combatting fraudulent communications in the digital age

Natalie Sullivan
Claims Solicitor

As cyber criminals become more sophisticated in their attempts to defraud law practices and their clients, it is important that solicitors regularly review and revise their risk management policies and procedures and ensure that all staff are adequately trained in identifying signs of suspicious activity.

A recent Lawcover claim highlights the importance of solicitors initiating the telephone call to their client to obtain verbal verification of bank account details before transferring funds.

The practice was engaged to act on the sale of a residential property. Upon settlement, the monies were deposited into the practice’s trust account in accordance with the client’s instructions. The same day, the practice emailed the client requesting their bank account details for distribution of the sale proceeds. The client responded by email providing the requested bank account details, however, the email was intercepted and redirected by a cyber criminal.

The following day, the practice received an email, purporting to be from the client, but which was in fact from the cyber criminal, providing a list of fraudulent bank account details for distribution of the settlement monies. At about the same time, the practice received an ‘internal’ email seemingly sent by an employee, but which was again sent by the cyber criminal. This email stated that the client had called and had requested that the practice telephone her on the number provided to verify the bank account details contained in the email which had just been received by the practice. The telephone number recorded in the email was the cyber criminal’s number.

Before any phone call was made by the practice however, the cyber criminal called the practice and spoke to a staff member to confirm the bank account details which had been included in the fraudulent email. The client was not known to the staff member, so the phone conversation did not raise any suspicion.

Acting on the fraudulent email and the phone call from the cyber criminal, the practice transferred the sale proceeds to the fraudulent bank accounts. Only half of the funds were able to be recovered.

This claim serves as a timely reminder that solicitors need to be ever vigilant in the face of increasingly sophisticated cyber criminals. Whilst verbal confirmation of bank account details has become a standard risk management practice, it is crucial that solicitors:

- Obtain and verify client contact details, in person if possible, at the commencement of the matter
- Initiate a telephone call to the client, using their verified phone number, to confirm bank account details before making any payments
- Ensure that the solicitor or staff member making the telephone call is familiar with the client
- If a client telephones the practice to verify bank account details, be vigilant in checking the identity of the caller and, if there is any uncertainty, arrange to call the client back on the verified phone number before proceeding with the confirmation.

Lawcover

WHEN MAKING A **PAYMENT**

Stop

Never rely on emailed account details

Double Check

Always check details in person or by phone

1. Make an outbound call
2. Use a known phone number (not the one on the email)
3. Be sure you know the person you are speaking to
4. Check the account details

Warn

Warn your clients and other payers to do the same