LEGAL PRACTITIONERS' LIABILITY COMMITTEE

February 2020

Beware the risk your client's email system may have been compromised

Our latest cyber claim story is a salutary reminder not to be complacent about payment directions received by email or be lured into thinking that because your IT system is secure, you are not at risk from cybercrime.

In this deceased estate matter, the estate had been wound up and most of the beneficiaries had received their money. The firm was just waiting on the last beneficiary to get advice from their financial advisor before receiving directions as to how the payment of funds to the last beneficiary should be made, and had been advised that information would be provided shortly.

The firm prepared a Statement of Trust Funds and Proposed Distribution Statement and sent these to the beneficiary by email for signing and return as authorisation to distribute.

A few days later the firm received an email from the beneficiary's email address with the signed Distribution Statement and instructions that:

"Just to let you know, my old account is going through end year auditing which I cannot received fund in it at the moment. I have now secured an alternate account and I want my proceeds distribution to be credited to my below account."

The firm made the payment into the nominated account without telephoning the sender (beneficiary) to verify the bank account details in the email.

Because the email was expected, because it enclosed a signed Distribution Statement, because it came from the beneficiary's email address and because both the firm's professional and accounts staff had not been adequately trained to **ALWAYS** verify email bank payment directions, the firm's guard against cybercrime was down.

As it turned out, although the email address did belong to the beneficiary, cyber criminals had infiltrated the beneficiary's email account and were monitoring emails to and from that account.

The criminals had:

- intercepted the law firm's email to the beneficiary enclosing the Distribution Statement and prevented it from going to the beneficiary's inbox

- forged the beneficiary's signature on the Distribution Statement

- sent a bogus email to the firm from the beneficiary's account with the forged Statement, and

- included false bank account details for payment of funds, together with a fraudulent explanation for the change of account at a branch of an interstate bank.

The explanation was clearly one which the firm should have been on guard to identify as suspicious, not only because of grammatical errors in the email but also because the explanation for funds not being able to be transferred into the beneficiary's existing account (i.e. it was undergoing audit) was patently non-sensical.

Unfortunately the firm's suspicions were not raised and it acted on the fraudulent email instructions, paying more than $600,000
it held on trust for the beneficiary into an account controlled by
cybercriminals. A few weeks later when the beneficiary followed the firm up to enquire when payment of funds would be received, the fraud was discovered and all
the money had been transferred out of Australia to overseas accounts and was unrecoverable.

The law firm had a misplaced belief they were protected from the risk of email cybercrime because their email system had very strong firewalls and spam filters in place. This case illustrates how wrong this can be, and that law firms are susceptible to the risk of receiving bogus email instructions from apparently legitimate email accounts which have been infiltrated and monitored by cybercriminals. In short, independent of the security status of your own email system, you are at risk your client's email account may have been compromised. You need to be mindful of that risk any time email payment directions are being provided so that your firm does not pay money to an incorrect account in breach of trust.

The message is clear – **there are no exceptions to the rule** – you must independently confirm emailed bank account details **every time**. Follow LPLC's recommended process and telephone and verify the account details on a known phone number for the person.

Every firm needs a clear, preferably written policy, that this is what will happen. Every staff member needs to be trained to follow this policy every time.

To prevent the delay in detection that happened in this claim, it is also a good idea to tell the recipient when the money is sent and ask them to confirm they have received the money as soon as possible.

For more information see our new Cyber Security Guide for Lawyers and our other cyber resources.