CALL FIRST TO AVOID CYBER FRAUD

When transferring money firms and their clients should always call first to check that account numbers are correct to avoid being victims of cyber fraud.

Does your firm have in place a clear procedure requiring staff transferring money to always call before they pay to verbally check payment details by reading out and reading back bank account numbers and BSBs? Are clients transferring money also warned to call to check account details before they pay? If you answered no, your firm is at risk of cyber fraud – and a claim – and should act now.

LPLC is continuing to see costly cases where this critical step is overlooked. In a recent claim, a Victorian law firm transferred more than $400,000 in trust money to bank accounts controlled by cyber-criminals instead of the intended beneficiaries of a deceased estate. In this case the firm called to confirm the transfer was taking place, but because they failed to undertake the critical step of verbally checking the accuracy of the account numbers, the payments were made to the cyber-criminal's accounts and were irrecoverable once the scam was discovered.

TIPS

- Never rely on emails or attachments providing bank account numbers.
- All firms should have a procedure requiring staff transferring money to always call before they pay to check account numbers by reading them out and back.
- On every matter clients should be warned to always call to check account numbers in the same way before transferring money.
- All staff should be trained in and understand the importance of reading out and reading back bank account numbers.
- Go to lplc.com.au/cyber for more information about cyber security for lawyers.

Timeline of events

17 June – Executor client emailed the law firm with bank account details for beneficiaries to distribute the deceased's estate.

24 October – Law firm's finance manager emailed the executor requesting further information for some of the bank accounts to make international money transfers.

29 October – The executor emailed the finance manager with original bank account details but failed to include the additional requested information. The finance manager replied by email that further information was needed. However, the email was intercepted and deleted by the cyber-criminal who had gained access to the executor's email account, so it was not received by the actual executor.

Impersonating the executor, the cyber-criminal then sent an email from the executor's email account saying that they would check the account details with the beneficiaries and confirm. Later that day the cyber-criminal sent through new account details for some of the beneficiaries which were accounts controlled by the criminal.

The finance manager then called the executor to confirm receipt of their email (which was really sent by the cyber-criminal) and that the transfer was proceeding with the bank details provided that day, but missed the critical step of reading out the account numbers to the executor and having them confirmed back. If they had done this, they would have realised then that something was wrong.

30 October – The finance manager then made payments totalling more than $400,000 to the cyber criminal's bank accounts. The funds were immediately transferred from the accounts by the cyber-criminal before the fraud was discovered.

Only about $50 was subsequently recovered by the banks. While banks will make recovery efforts, the speed of electronic fund transfers, and increasing use of cryptocurrency accounts by cyber-criminals, means there is a very small window of time to act before the cyber-criminal moves the money and it's unrecoverable. Banks are not obliged to reimburse the stolen funds when this occurs.

Key takeaways and risk management recommendations

The purpose of payment verification procedures should be well understood and followed by all staff in your firm who handle the transfer of money or work on client matters.

Firms and their clients should never solely rely on bank account details sent by email. Before transferring money, always call on a previously known number to verify the account numbers by reading aloud both the account BSB and account number and ask for it to be read back to you. Write down the details and check it against what you have been provided by email.

When calling, don't use the contact details given in the email or other document providing the account details, as it may be the cyber criminal's telephone number. Always independently source the phone number and only call once you are confident the number you are calling is correct. This is particularly important when dealing with third parties or clients you don't know well.

Write a file note about the call confirming the bank account details and place this directly on your file. Don't rely on emails confirming that the verification procedure has taken place – LPLC has seen many cases where the confirming email has been fraudulently sent by a cyber-criminal impersonating staff. Call and also check the file to ensure that it's been done.

LPLC is continuing to see client funds being stolen and claims arising where clients themselves have transferred money to the wrong account. It is important that firms tell their clients to be cyber vigilant and always call and verify account details by reading aloud and reading back account details. LPLC has produced a sample client brochure on its website containing key messages for clients about how to protect themselves that firms can use/adapt for this purpose.

It is critical all staff are trained in and understand the importance of reading out and reading back account details and the firm's procedure. Using real life examples such as the story above can assist with understanding why this step is so important and can never be missed.

If your firm is insured with LPLC and would like further information or assistance with how to go about implementing verbal verification procedures and staff training, contact LPLC at 9672 3800 or lawyersrisk@lplc.com.au. ■

This column is provided by the **Legal Practitioners' Liability Committee**.
For further information ph 9672 3800 or visit www.lplc.com.au.