



Electronic Funds Transfer warning - everything is not always as it seems

Date: Monday July 13, 2020

The recent New South Wales Supreme Court decision in [Deligiannidou v Sundarjee \[2020\] NSWSC 437](#) is a cautionary tale for anyone sending money electronically, particularly large sums of money in property transactions. This case refers to a purchaser's payment of a deposit on a property purchase, by way of an electronic funds transfer (EFT) into a real estate agent's trust account.

An initial deposit was paid by EFT

As the purchase Contract was subject to a cooling-off period, the purchaser paid an initial 0.25% deposit on exchange, with the balance of \$54,600.00 due to be paid to the Vendor's agent 11 days later, on 12 February 2020.

The initial deposit was paid by EFT to the trust account of the vendor's agent. The purchaser was supplied with the BSB and account numbers provided via email from the vendor's agent.

Balance requested by email

On 9 February 2020 (three days before the final payment was due), the purchaser received an email which appeared to be from the vendor's agent, attaching an invoice and requesting the balance of the deposit be paid. As in the previous email requesting the deposit transfer, BSB and account numbers were provided.

This email was sent to the purchaser as part of an email chain which purported to include earlier emails from the vendor's agent.

Trust account details altered

However, the trust account BSB and account details in this email chain had been changed from the original BSB and account numbers to reflect those in the invoice attached to the email.

The purchaser transferred the \$54,600.00 to the new/revised account referred to in the email and attached invoice.

Two days after the due date for payment, the vendor's agent contacted the purchaser advising that the money had not appeared in the trust account.

Agent's email account had been hacked

The agent's email account had been hacked and the BSB and account numbers had been altered to direct funds to the account of the hacker.

Protecting your electronic funds transfers

The agent and purchaser could have avoided the fraudulent transfer with a simple phone call by the purchaser to the agent, to confirm the BSB and account number for transfer of the \$54,600.00; particularly given it was different to the initial banking details provided.

To avoid electronic funds transfer (EFT) fraud, it is our firm's policy to always call our client, or other party, providing account details over the phone and then by email to confirm. It may be a good idea for you to consider the same when transferring funds electronically.

Contacting E&A Lawyers

For more information or to arrange a consultation with a lawyer, you can call or email us.

[02 9997 2111](tel:0299972111)

info@ealawyers.com.au

This article is of a general nature and should not be relied upon as legal advice. If you require further information, advice or assistance for your specific circumstances, please contact E&A Lawyers.