LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Risk video bites

Risk video bites – Fake bank account details

Presenter: Heather Hibberd

More and more lawyers and their clients are becoming victim to fake emails. The key risk areas are conveyancing, wills and estates, sales of business and family law – areas where lawyers are holding and transferring large sums of money for their clients.

The key message is you CAN NOT rely solely on bank account details sent in an email. That email may have been intercepted by a fraudster and the bank account details changed.

If you receive bank account details from your client in an email you must speak to your client and confirm the details. NO matter how well you know the client and no matter how authentic the email looks. NO exceptions.

Our cyber poster [show image] explains the steps you have to take and every firm needs to have that poster on the wall to remind them. You can down load copies at our website or we can send you A3 versions if you email us.

But what about clients or others who are paying money into your firm's trust account? If your client receives a fake email purporting to be from your firm directing them to pay money into a fraudster's bank account, will THEY know to check if it is fake?

In a recent claim our insured firm acted for vendors of property in a private sale. The practitioner's secretary emailed the firm's trust account details for payment of the deposit to the purchaser's solicitors.

The next day, the purchaser's solicitors received an email purporting to be from the practitioner advising '*of a little error in the bank details sent earlier*' and setting out '*the corrected details of our trust account*'.

With the benefit of hindsight, that email had some hallmarks of being a fake –

- although purporting to be from the practitioner, the footer was that of his secretary
- the font was different

- the greeting was unusual and
- the corrected details appeared in a different font.

Notwithstanding these hallmarks, the purchaser's practitioner raised no query and did not telephone the vendor's practitioner to verify the apparent change of account details. The deposit was then paid into the fraudster's account and disappeared.

A day or two later when the vendor's practitioner had not received the deposit, the purchaser's solicitors emailed a bank transaction group report to him to show where the money had been delivered. The fraudsters also intercepted this email and changed the bank account details to incorrectly show payment having been made into the right account. The significance of this is that it further delayed discovery of the fraud.

Two days later, the practitioner again contacted the purchaser's solicitors and the fraud was discovered. Happily, through swift action in immediately contacting the receiving bank, the account was frozen and the funds were recovered. It was a near miss.

It turned out that the vendor's practitioner's email account had been hacked enabling the fraudster to access and create fake emails which duped the purchaser's solicitor.

To avoid these type of frauds, we recommend that your firm tells clients at the start of every matter:

- your firm's trust account details are in your engagement letter and you will not change those details
- if the client receives an email from your firm containing changed trust account payment details, they must telephone the firm to verify the position, and not to respond to the email.

Put this information in your firm's standard engagement letter. Consider providing clients with:

- a cyber security brochure like the one on our website [image https://lplc.com.au/client-resources/cyber-security-protect-client-brochure/]
- a warning in other communications from your firm such as newsletters and email signatures.

Finally, discuss this important issue with colleagues and other firms, so everyone is aware of the risks.

Thanks for watching.