Impersonation fraud – Saved from a costly mistake

Background

A law practice was retained to act in the sale of a large property in rural NSW. The practice held Professional Indemnity Insurance (PII) cover of $2 million as well as Top Up insurance for an additional $3 million cover. The practice was also a member of the Law Society of NSW (Professional Standards) Scheme (Scheme).

The solicitor had been corresponding with the client via email, settlement occurred and funds of $3.2 million were paid into the practice's trust account pending further instructions from the client. Unbeknownst to the practice, the email exchanges between the solicitor and the client were being monitored by a fraudster. Knowing that a large transaction had taken place, the fraudster called the practice purporting to be from their bank's fraud team (impersonation fraud). The fraudster used technology to make it appear as if the call was coming from the bank's phone number (call spoofing) and claimed to be investigating a suspicious transaction. The fraudster was able to gain enough information from the solicitor to gain access to their trust account and steal the $3.2 million.

The Claim

The client brought a claim against the practice for breach of trust seeking $3.2 million in damages. Under the Scheme, liability is limited to $1.5 million for most claims, however, the Scheme does not cover claims for breach of trust.

Top Up Insurance

Fortunately, the practice purchased an additional Top Up layer of $3 million cover, to a total coverage limit of $5 million. This meant the full $3.2 million claim was covered ($2 million under the primary PII policy and $1.2 million under the additional Top Up cover).

The practice principals avoided personal exposure to amounts claimed above the $2m primary limit by purchasing additional cover.

The primary $2 million policy limit and the Scheme may not always be enough protection in every instance. The Scheme has certain limitations and exclusions (refer to page 10) that should be considered, particularly if a practice is dealing with high value transactions or large matter volumes. Every practice should evaluate their risk exposure regularly and consider if Top Up insurance is needed.

For risk management tips relating to cybercrime and impersonation fraud see page 13.

Keep your accounts safe

Practices should ensure that adequate processes and procedures are in place to safeguard against fraudulent attacks and access to sensitive information.

Remember

Stop

- Don't rely on the phone numbers provided in a text message or email
- Don't give information like passwords, financial information, bank numbers, security codes, PINS, tokens etc. to anyone over the phone or via text or email
- Don't click on any links in text messages or emails if you're unsure
- Hang up if you receive a call from someone claiming to be from a bank asking you to transfer money or for sensitive information

Check

- If you receive an email, phone call or message from someone who says they are from your bank, ask for a reference number and then contact your bank separately using your banking app or a phone number you have sourced from your banking app, bank website, bank statement or bank card
- Always call to confirm emailed bank account details before transferring funds. Do not rely on the phone number in the email

Act

- Act quickly if you have transferred funds and/or given a scammer information or access to your account - immediately report the cyber incident to the security team of any involved banks, and contact Lawcover on **1800 4BREACH** (1800 427 322)