Cyber assisted fraud – still a substantial threat

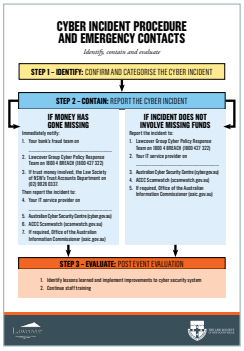
Milica Vukancic
Claims Solicitor

Lawcover continues to see cyber assisted fraud claims, particularly in relation to payment redirection fraud and a loss of client funds.

These frauds are perpetrated by cyber criminals that are obviously familiar with the nature of legal transactions. They often involve business email compromise attacks, where either the law practice or client's IT system is hacked, information is collected about the target, an impersonation email is sent, usually requesting to change bank account details and funds are transferred unknowingly to the cyber criminal.

Fraudulent redirection of funds out of the practice's trust account or directly from a client often strike at a critical stage of a property transaction. This results in the client potentially being placed in a position of contractual breach.

It is important that all solicitors have robust cyber security measures in place to secure their practice and ultimately their reputation by preventing cyber breaches.



Cyber Incident Procedure - for Law Practices

If your law practice suffers a cyber breach, this is your step-by-step response guide.

Click here for more information.

Risk management tips

- Add your trust account details to your Costs Agreement. Inform your client that these details will never be changed by email
- Before making a payment take these important steps:
  - Never rely solely on emailed account details to make a transfer or payment
  - Always check details in person or by phone:
    i. Make an outbound call using a known phone number (not the one on the email) to check the account details
    ii. Be sure you know the person you are speaking to
    iii. Check the account details
  - Warn your clients and other payers to do the same
- Speak with cyber security experts to ensure that your computer and IT systems in your practice are well protected
- Include multi-factor authentication to computer systems to improve security

If you suspect your system has been compromised:

- Contact the cyber risk crisis management team on **1800 427 322** to notify them of a cyber incident under the Lawcover Group Cyber Risk Policy
- Contact the affected client and advise them to urgently notify their bank to intercept the transaction or assist in recovering the funds
- Undertake an immediate audit of your files and contact all clients with upcoming settlements or other payments. Warn them not to rely on email requests for the transfer of funds without first confirming the instructions, preferably in person, or at least by phone, using a verified contact phone number
- Conduct an audit of recent settlements to make sure that an earlier fraudulent interception of funds has not occurred

If you experience a cyber incident

Call 1800 4BREACH
(1800 427 322)

Visit Lawcover's website for Cyber Risk Resources and a Cyber Security Guide
lawcover.com.au/resource-centre/