

Private & Confidential

28 May 2025

Update to investigation into cyber incident

Following our email yesterday about the recent cyber incident, we wanted to provide you with a further update.

We understand that this news has caused some concern, so we wanted to share some more details to help address some common questions.

Information involved

We would like to assure you that the disclosed data included very limited banking information relating to a small number of third parties, who have been directly notified.

If you have not been directly contacted by the Legal Practice Board regarding your banking information, it was not contained in the disclosed data and there is no action you need to take.

As outlined in yesterday's email, we are working as a priority to determine the full nature and extent of this incident, and whether any other information was accessed. We will provide further updates as we know more.

We do not have any credible evidence to confirm at this point of our investigation that the unauthorised third party possesses any other Board data. Nevertheless, to ensure we are taking all available action in response to this incident, we have also obtained an injunction to prevent any access, dissemination or sharing of data impacted by this incident.

Online services

We are also working to restore access to our online services as soon as possible. In the interim, we are processing applications for practising certificates manually.

We apologise for any inconvenience this may cause. The practising certificate form can be accessed on our website - <https://www.lpbwa.org.au/login?returnurl=/service-hub> – and should be submitted to enquiries@lpbwa.com

While our online payment system is unavailable, we will directly contact individuals where required to arrange payment, at the rate that applied when the form was submitted.

Please be assured, if you submitted your form via our online portal prior to 21 May 2025, this has been received and there is no action you need to take.

Further questions

We hope this information helps to address the questions you may have. We have also provided some further guidance and general cyber safety information below you may find helpful.

We have dedicated response team available to answer any other questions about the incident who can be contacted on our Helpline on 08 7070 2413 or by emailing incident@lpbwa.com.

The Board will continue to provide further updates as we know more – thank you for your understanding and patience as we work through this.

I'm concerned about bank account information being impacted

We would like to assure you that the bank account information in the disclosed correspondence related to a very small number of third parties, which have been notified.

The most likely risk associated with access to this type of information is for scams to appear more legitimate. It is important that we are all aware of the risk of scams or phishing emails at this time.

Were my trust account details impacted?

We have no evidence at this time to confirm any impact to trust account details.

I'm still concerned about my bank/payment details

A BSB and account number does not present a direct misuse risk as, alone, they do not allow unauthorised access to your bank account. However, the BSB does identify who the financial institution is, which may make impersonation scam attempts appear more legitimate. It is important that we all practice extra vigilance against the risk of scams.

Should you have any concerns, you can consider the following:

- review your transaction history and bank account statements for any suspicious activity;
- contact your bank to report this event and flag any suspicious activity identified;
- where available use two-step authentication – such as SMS codes to your mobile phone;
- check your credit report yearly (this alerts you to any attempts to open a credit account in your name). Information about obtaining a credit report is provided below; and
- never respond to, open or click on links in emails purporting to be from your bank (it is always safer to call).

Is my information safe?

We do not have any credible evidence to confirm at this point of our investigation that the unauthorised third party possesses any other Board correspondence, although we are reviewing what could have been accessed as a priority.

As communicated to our stakeholders, a small amount of correspondence confirmed as taken from our IT environment has been disclosed. This data included correspondence which primarily contains limited contact details and internal operational and resourcing information, as well as bank account information for the Board and a small number of third parties, who have been directly notified.

The most likely risk associated with access to this type of information is for scams to appear more legitimate. We therefore recommend you are extra vigilant against the risk of scams.

We provide further guidance on this below.

General cyber security guidance

Be aware of scams

We encourage you to stay alert to the possibility of phishing emails and scams, as these are common risks associated with unauthorised access to personal information and cyber events. If you receive an unexpected email, call, or message, especially one asking for personal information or money with a sense of urgency, or with obvious spelling and grammatical errors, be cautious. Verify the sender's identity through official channels before responding and sharing any information.

Check email addresses and links

Look closely at the sender's email address and any links provided. Scammers often use addresses that look very similar to legitimate ones, sometimes with just a single letter changed in the company name. Carefully check the sender address and hover over any links to see the actual address before clicking. Practice the same caution with websites - if you are suspicious of a website address, do not click on the link or provide login details.

Use strong, unique passwords

Create strong passwords using a mix of letters, numbers, and symbols. Avoid using the same password on more than one account. Consider using a password manager to keep track of them.

Enable Multi-Factor Authentication (MFA)

Whenever possible, enable MFA on your online accounts for an extra layer of security, including on your email, banking and social media accounts. MFA typically involves receiving a code on your phone or email that you must enter in addition to your password.

Secure your devices with anti-virus software

Use antivirus software and keep it updated. Ensure your devices are also protected with strong passwords or biometric security features.

Learn more about cyber safety

Read the Australian Competition and Consumer Commission's Scamwatch guidance for protecting yourself from scams here: <https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams/>. You may also want to read the OAIC's tips for further guidance about protecting your identity: <https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to-protect-your-privacy/>.

Yours sincerely

Legal Practice Board