Keylend Suffers Eligible Data Breach

On Thursday 23 April 2026, Australian Associated Advisers Pty Ltd trading as Keylend (**Keylend**) discovered that an unauthorised third party had used a single Keylend user's account and email (**Mailbox**) to send malicious phishing emails to third parties (**Incident**).

Upon becoming aware of the phishing emails sent on 23 April 2026, Keylend immediately contained the Incident removing the unauthorised third party's access to the Mailbox. Keylend sent emails to recipients of those phishing emails alerting them not to interact with the phishing email, and to delete that email.

Keylend also immediately commenced an investigation into the Incident, and this work is ongoing.

Keylend is aware that additional phishing emails may have been sent using the Mailbox. Keylend also considers that a copy of the Mailbox content may have been copied by the unauthorised third party, and so is undertaking a full review of the mailbox content so that notifications can be made to any and all affected individuals at risk of serious harm.

Keylend is monitoring the dark web in relation to the Incident, and no evidence has been identified to date on the dark web relating to the mailbox content or the Incident, and this monitoring is ongoing.

The Incident has been reported to the Office of the Australian Information Commissioner and the Australian Securities and Investments Commission.

Data that was compromised

At this time, Keylend knows that the Mailbox contacts were used to send the phishing emails and is undertaking a full review of the mailbox content to identify the other information affected.

Our focus is to minimise any risks that this Incident may cause to you, and we will let any affected individuals at risk of serious harm know once that investigation has been completed.

What should you do?

Ensure you do not interact with any phishing email that Keylend has notified you about and ensure these have been deleted.

Please maintain your usual practices of:

- being wary of any unexpected or suspicious communications, scam emails, text messages or phone calls, that purport to be from Keylend or any person or company that you know or trust (and if in doubt, contact that person or company back on their publicly listed official contact channels);
- ensuring you have suitable security on your online accounts and devices, including the use of multi-factor authentication for your email and other online accounts;
- regularly changing your online passwords (using strong passphrases – see https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases.
- remaining vigilant to any misuse of your personal information and familiarise yourself with the information on online safety, cyber security, scams, identity theft and other online risks at the following government agency websites:
    - https://www.cyber.gov.au/threats
    - https://www.scamwatch.gov.au/types-of-scams

Any affected individuals identified as part of the review of the Mailbox content will be contacted directly and notified of any additional recommended remedial action.

Contact Keylend if you need more information

We are sorry that this Incident has occurred. We have established a dedicated support line on (08) 7092 1333, open 9am - 5pm AEST Monday to Friday (excluding public holidays). Please get in touch with us if you have any questions or concerns, we are here to help. Alternatively, you can contact the independent IDCARE service as described in more detail below.

IDCARE Service

Keylend has partnered with IDCARE, Australia's national identity and cyber support community service.

IDCARE's expert Case Managers can assist you with concerns about personal information risks or situations where you believe your information may have been misused.

IDCARE's services are provided at no cost to you where you are affected by this Incident.

To speak with a Case Manager, complete the online Get Help form at www.idcare.org or call 1800 595 160. Specialist Case Managers are available 7am–7pm AEST, Monday to Friday (excluding public holidays).

When engaging with IDCARE, please use the referral code provided to you by Keylend, in order to unlock IDCARE's services.