QUEST
APARTMENT HOTELS
A Member of The Ascott Limited

AS LOCAL AS YOU LIKE IT.

DATA BREACH - FREQUENTLY ASKED QUESTIONS

What happened?

On 17 August 2026, Quest identified an outage on its website. Investigations into the outage confirmed that a malicious attack had occurred after a threat actor exploited a vulnerability in a third-party service provider's software and gained access to Quest's environment. We then took immediate steps and contained the incident. Quest's systems are secured.

The incident affected limited customer records to July 2025, which our third-party service provider had left on that environment. We are progressing our investigation with our third party service provider regarding this incident.

What personal information was affected?

Our investigation has confirmed that the affected data primarily contained booking information and personal information relevant to an individual's stay with us, including:

- names;
- addresses;
- contact details; and/or
- personal preferences.

In a limited number of cases, the affected data also included:

- date of birth;
- driver's licence numbers (excluding image of passport, expiry dates, and licence card security numbers);
- passport numbers (excluding image of passport and expiry dates);
- credit card number and expiry date (excluding CVV);
- credit card number, expiry date and CVV;
- credit card number (that has expired or did not have an expiry date);
- Medicare number;
- NDIS number; and/or
- vehicle registration number.

Not all categories of information apply to every affected individual. We are contacting individuals whose personal information falls within these additional categories as they are identified directly.

If you do not hear from us soon, your personal information was not affected by the incident.

How will I know if my personal information has been compromised?

We have directly emailed those affected individuals whose email details are available to us, advising on the types of personal information impacted by the incident. Please check your spam or junk folder to confirm.

We are also taking steps to inform other affected individuals via SMS or post, to the extent we do not have their email addresses.

We will provide further information to the affected individuals as and when necessary while we progress our forensic analysis.

What steps have we taken in response to the incident?

We have made further cyber security improvements to reduce the risk of this type of incident happening again with assistance from our third-party service providers.

We disclosed this incident to the Australian Cyber Security Centre and the Office of the Australian Information Commissioner. Given the criminal nature of this incident, law enforcement authorities were also notified.

What should I do if my personal information has been compromised?

Some immediate and general precautionary steps that you can take include:

DO NOT:

- open any suspicious texts, pop-up windows, emails or social media messages from unknown senders;
- click on suspicious links or open unusual attachments from individuals or organisations you do not know, even where they may purport to be from Quest;

DO:

- be and remain vigilant in communications and other activities online for any unusual activity, e.g., phishing or scam emails;
- to help protect against fraud, look to reputable sources such as:
    - https://www.scamwatch.gov.au/
    - https://www.cyber.gov.au/
- be cautious when answering calls from unfamiliar numbers, or talking to or following instructions from someone you do not know.

In addition, if we have notified you that your personal information falls within the additional categories above, you may wish to take the following additional steps (as relevant):

- **Credit card statements:** Review your recent transaction history and credit card statements for any suspicious activity, and contact your bank to report the breach and flag any suspicious activity identified.
- **Consider a credit report ban:** Consider requesting a credit report ban in place to 'freeze' access to your credit file, so that Credit Reporting Agencies are not able to disclose any personal information from your consumer credit file to any credit providers unless you provide written consent for them to do so or if they are required by law. You can lift this ban if you need to apply for credit later on. To do so:
    - Equifax: Please go to: https://www.equifax.com.au/personal/help-centre/credit-report-ban/ban-my-equifax-credit-report and fill in and submit the form.
    - Experian: Please go to: https://www.experian.com.au/consumer/request-a-ban and fill in and submit the form.

  As an additional measure, you can apply for an annual free credit report from any one of the consumer Credit Reporting Agencies below:
    - Equifax https://www.mycreditfile.com.au/products-services/my-credit-file
    - Experian http://www.experian.com.au/consumer-reports
- **Consider contacting Services Australia:** Consider contacting Services Australia to advise of the unauthorised disclosure of your Medicare card number so that, if required, a new or replacement Medicare card and number can be issued and relevant records updated. Services Australia's Scams and Identity Theft Helpdesk can be reached by calling 1800 941 126 or via email at reportascam@servicesaustralia.gov.au.
- **Consider contacting NDIS:** Consider contacting NDIS to advise of the unauthorised disclosure of your NDIS number so that, if required, a new or replacement NDIS number can be issued and relevant records updated. NDIS' Fraud Reporting and Scams Helpline can be contacted by calling 1800 650 717.

- **Consider contacting your State or Territory roads authority:** Consider contacting your State or Territory roads authority to understand what additional steps you can take.
- **Passport:** Following the advice of the Australian Passport Office, we understand that if your Australian passport number was compromised in this data breach, your passport is still safe to use for international travel. The Australian Passport Office has adivsed that your passport number cannot be used to obtain a new passport and that robust controls are used to protect passports from identity takeover, including sophisticated facial-recognition technology.

What support is available to me?

Protecting the privacy and security of our customers is extremely important to us. We encourage you to contact us at privacy@questapartments.com.au.

We will continue to provide updates on this dedicated page.

Where can I find more information?

We will provide updates on this dedicated page.

You can also contact us at privacy@questapartments.com.au.

How do I know emails I receive from Quest are legitimate?

Our emails will come from a domain that ends in questapartments.com.au.

Please check that the email you have received has an email address with questapartments.com.au.

Do not rely on the display name only as it can be made to look like the sender is Quest.

Please be aware of any misspellings or similar-looking domain names – these are indications that an email may not be legitimate.

How do I know an SMS I receive from Quest is legitimate?

SMS messages from Quest relating to this incident will be sent from +61 (485) 095 177 or +61 (468) 153 778. Any legitimate SMS from Quest will direct you to our website at www.questapartments.com.au or to contact us at privacy@questapartments.com.au. We will never ask you to provide passwords, credit card details, or other sensitive information via SMS.

If you receive a suspicious SMS that claims to be from Quest, do not click any links or reply. Instead, contact us directly at privacy@questapartments.com.au to verify its legitimacy.

Who can you contact for more information?

If you have any further questions, please contact us at privacy@questapartments.com.au.