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.

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:

QUEST
APARTMENT HOTELS
A Member of The Ascott Limited

AS LOCAL AS YOU LIKE IT.

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.

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.

Who can you contact for more information?

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