Flight Centre Travel Group discloses possible customer data exposure via third-party booking system



Flight Centre Travel Group says unknown persons may have accessed customer records in a third-party accommodation booking system, mostly names, with limited passport and health data in rare cases. Payment data has not been affected so far.

- The incident involves unusual activity in a third-party accommodation booking system used by the Flight Centre brand, Travel Associates, Cruiseabout and some independent agents.
- Most accessed records hold only names, some with basic travel details; a very small share may include limited passport details, contact details, birth dates or, rarely, health or mobility information.
- No access to credit card, payment or bank account details has been found to date.
- Flight and corporate travel bookings are reported as unaffected.

> - The company is working with the vendor and Mandiant, has changed authentication keys and credentials, and is notifying authorities.

Flight Centre Travel Group (FLT), based in Brisbane, told the Australian Securities Exchange that it is investigating unusual activity in a third-party system used to book accommodation. The system serves the Flight Centre brand, Travel Associates, Cruiseabout and some independent agents.

What is known

FLT believes a significant number of customer records in the affected system may have been accessed, though it is not yet clear how many were actually extracted. An initial review indicates most records contain only names, sometimes with basic travel information. A very small percentage may include limited passport details, email addresses, phone numbers, birth dates or, rarely, health or mobility information.

The company reports no access so far to credit card, payment or bank account details. Flight bookings and corporate travel bookings are said to run on other systems and are not affected.

Response and wider context

FLT activated incident response, worked with the third party to contain the activity, changed authentication keys and credentials, increased monitoring and is notifying the relevant authorities. It is working with the vendor and Mandiant to establish scope. Customers are advised to treat unexpected emails, calls or messages about bookings with caution and not to click links, open attachments or share personal or payment details.

The source notes this follows other booking-related incidents, including a Booking.com warning in April and a breach at accommodation software provider RMS Cloud, after which guests received phishing messages.

Why it matters for Saudi institutions

The case shows how a single supplier platform can expose data belonging to several brands. Organisations that rely on travel or hospitality platforms for staff, customer or delegate bookings should check what personal data those suppliers hold and how quickly they would be told of an incident.

What to do now

1. Inventory third-party travel and accommodation booking platforms used for staff and delegate travel, and the personal data each one holds, including passport data.
2. Ask these suppliers to confirm in writing whether they are affected and how they will notify you of incidents.
3. Remind travelling staff and executives to treat unexpected messages about bookings as possible phishing and to verify through known channels.

4. Confirm supplier contracts require timely breach notification and support PDPL obligations on incident reporting.
5. Review credential and API key rotation procedures for supplier integrations so they can be executed quickly after an incident.