THREAT BRIEFING · 4 NOVEMBER 2026

The Amadeus Breach



How one travel tech supplier exposed passengers at Asia’s biggest airlines, and how to respond

ZNexora Tech Threat Briefing

znexoratech.com

In this briefing

What happened
Booking data exposed through Amadeus

How it happened
A supply chain breach, not an airline hack

Protect yourself
Six steps for affected travellers

Manage supplier risk
Remediation and prevention for organisations

7+

airlines affected
including JAL, ANA, Cathay Pacific and Singapore Airlines

Figures as of 4 Nov 2026

Reported impact by airline

Airline	Reported impact	Sensitive extras
Japan Airlines and JTA	About 92,000 customers	About 2,000 with passport numbers
Cathay Pacific	About 53,000 bookings	Travel documents for a subset
Singapore Airlines	About 46,000 booking records	Names, itineraries, booking classes
ANA	About 37,800 customers	About 1,700 with passport details
Korean Air, Asiana, Malaysia Airlines	Not disclosed	Under investigation

Three years of exposure, two weeks of disclosures



Aug 2023

Affected period begins

Sep 2026

Affected period ends

20 Oct

Amadeus notifies airlines

23–30 Oct

JAL, ANA, Cathay disclose

3 Nov

Singapore Airlines: 46,000

Amadeus has not disclosed how many airlines or passengers are affected in total.

How it happened



Shared supplier
Many airlines use Amadeus

System account
Its credentials were used

Booking display
A weakness exposed data

Data viewed
Names, bookings, some passports

Phishing risk
Real details, fake messages

No payment card data or account passwords were exposed, according to Amadeus and the airlines.

Why it matters: third-party risk



Shared dependency

One supplier holds passenger data for many airlines



Airlines not breached

Their own systems were safe, yet customers were affected



Not the first time

SITA in 2021 affected about 1 million ANA and 920,000 JAL members



Vendor reviews

Korean Air will inspect every vendor handling personal data

Protect yourself: six steps for travellers

Expect fake messages

Scammers may quote your real booking

Use the official app

Never pay or log in via message links

Guard your passport

Airlines never ask for scans by email

Secure mileage

Unique password and two-step verification

Check the notice

Is your booking in the affected period?

Report phishing

To the airline and antiphishing.jp

Organisations: remediate now



Get the facts

Systems, data, period, fixes

Find affected customers

Most sensitive data first

Notify and warn

Customers and regulators

Rotate credentials

Anything shared with the supplier

Monitor

Brand phishing and loyalty fraud

In Japan, serious breaches must be reported to the Personal Information Protection Commission.

Prevent: managing supplier risk

- [ ] Inventory of every supplier holding customer data
- [ ] Share only the data each supplier needs
- [ ] Security and 72-hour breach notice in contracts
- [ ] Logging and alerts on access to your data
- [ ] Supplier system accounts: unique, rotated, least privilege
- [ ] Supplier breaches included in incident response drills

Key takeaways

- The airlines were not hacked, but their supplier was.
- Travellers: expect convincing phishing using real booking details.
- Organisations: know your suppliers and hold them to clear security rules.

Read the full briefing at znexoratech.com