KILLSWITCH · ISSUE #8 · 4 NOV 2026

One supplier login. Three years. Nobody noticed.

Your supplier's system account is part of your attack surface.

Killswitch rating: Review supplier accounts this month

By Emmanuel Aigbehi Walstra

One supplier login. Three years. Nobody noticed.

JAL: traces of outside access from 10 Aug 2023 to 23 Sep 2026, in Amadeus's passenger service system [1].

- Cathay: access used "login credentials assigned to its system account" [4].
- Airlines were told weeks after the last trace [1][4][5].

Who has said what so far

1 **JAL [1]**

About 92,000 customers; about 2,000 with passport and contact details

2 **ANA [2]**

About 37,800 customers; about 1,700 with passport and contact details

3 **Cathay [4]**

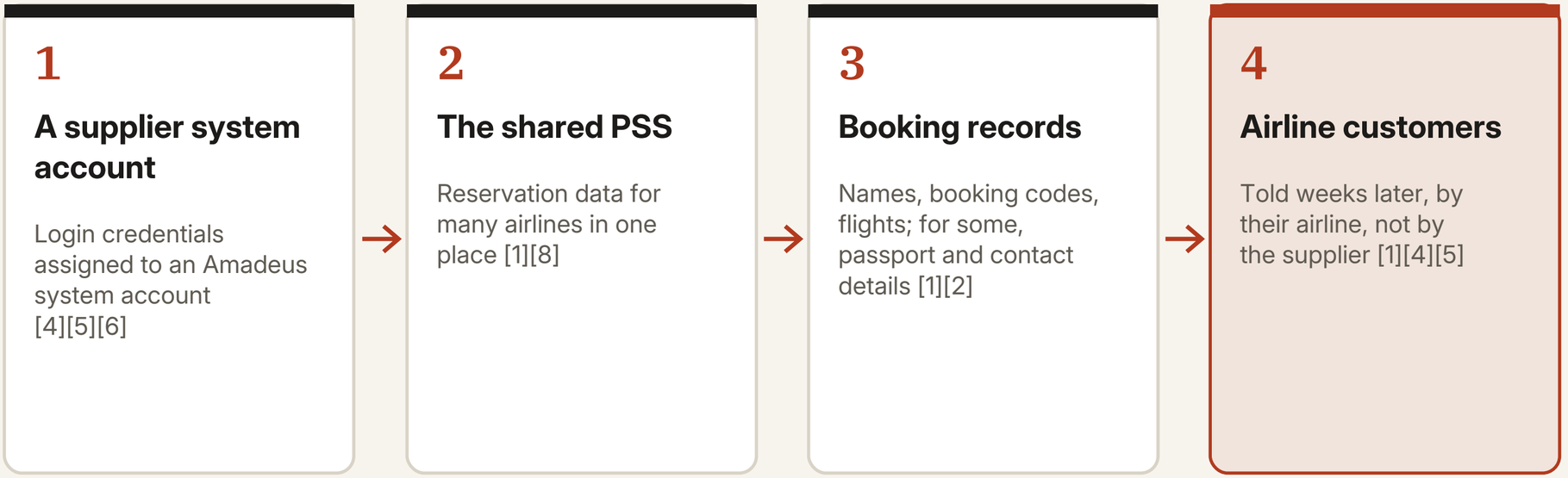
About 53,000 bookings

4 **Star Flyer [3] · Korean Air, Asiana [5] · Malaysia Airlines [15]**

No count published yet

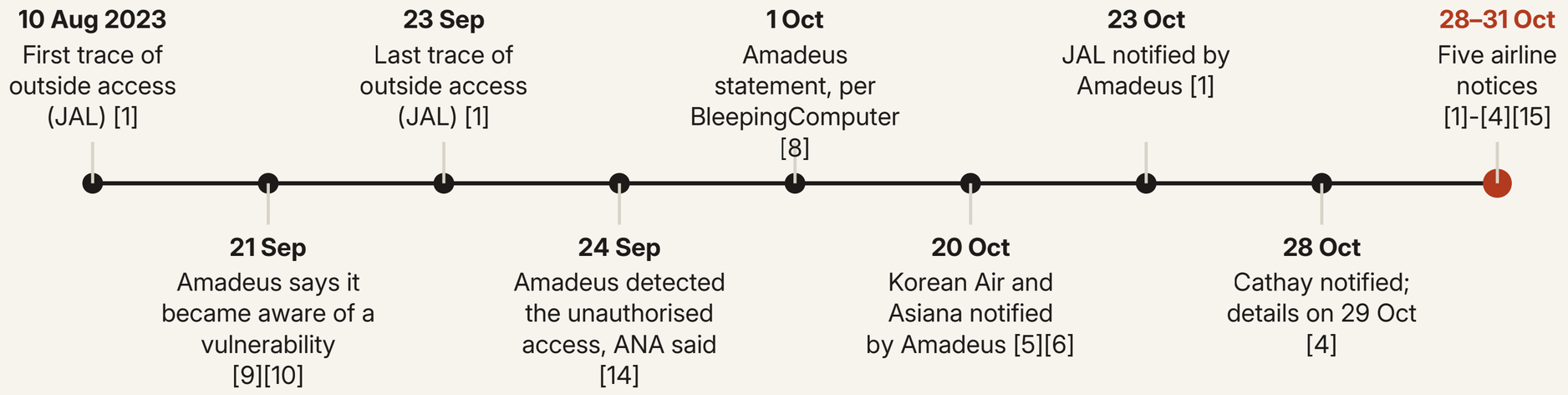
Each airline's own count. JAL and ANA count customers, Cathay counts bookings, so the figures do not add up to one total.

Not the airlines' systems. The supplier's account.



Access as described by Cathay [4], Yonhap [5], Asia Business Daily [6]. Heap dump: heise [9][10]; same route not confirmed.

Three years in. Five weeks to tell.



JAL dates the traces [1]. Amadeus dates per heise [9][10], Kyodo [14] and BleepingComputer [8]. Dates 2026 unless shown.

What Amadeus has said

- Says it became aware on 21 Sep of a "potential vulnerability" in a booking display environment [9].
- BSI passed a coordinated-disclosure report to the vendor; no date given [10].
- Its own statement: certain booking data "was accessible through the vulnerability"; it does not say it was accessed [16].
- "No indications" of ransomware use [7]. No count of airlines [7][8].

No card or payment data. So far.

- JAL, ANA, Star Flyer: no credit card numbers or passwords [1][2][3].
- Cathay, Malaysia Airlines: no evidence payment data was accessed [4][15].
- No evidence of misuse so far: JAL; Cathay, relaying Amadeus [1][4].
- Own systems not breached: Cathay, Korean Air, Asiana, Malaysia Airlines [4][5][6][15].

Five controls for supplier-held data

1. **Inventory supplier accounts**
   Every system and service account a supplier uses on your data
2. **Rotate and bind them**
   Short-lived credentials, MFA or workload identity, no shared static secrets
3. **Ask for the logs**
   Contract for access logs on your records, and review them
4. **Set a notification clock**
   Days, not weeks, from supplier detection to your notice
5. **Rehearse the supplier breach**
   Customer notice, regulator notice and phishing warning, ready to go

Killswitch's own list.

Where this lives in your frameworks

Supplier accounts	A.5.17, A.5.18 · NIS2 21(2)(i), (j)
Supplier security	A.5.19-A.5.22 · NIS2 21(2)(d), 21(3) · DORA Art. 28-30
Detect odd access	A.8.15, A.8.16
Respond and notify	A.5.24-A.5.26 · NIS2 21(2)(b)

Killswitch's own mapping. Check ISO titles against your licensed copy. DORA applies to financial entities, not airlines [13].

ISO/IEC 27001:2022 [11] · NIS2 [12] · DORA [13]. Killswitch mapping.

09 · STILL OPEN

What we don't know yet

- One route or two: heap dump [9] and system-account login [4].
- How the login was obtained.
- Which airlines: no list from Amadeus [7][8].
- Final counts [3][5][15].

Do this month

- List every supplier holding your customer data, and its accounts.
- Ask how those credentials are issued and rotated.
- Get the access logs for your records.
- Put a notification clock in the contract.
- Rehearse a supplier-breach notice.

SOURCES

Sources (1/2)

[1] Japan Airlines: Regarding Unauthorized Access to Amadeus Passenger Service System and Our Response (first published 28 Oct, updated 30 Oct 2026)
[2] ANA: notice on unauthorized access to the Amadeus passenger service system
[3] Star Flyer: notice on unauthorized access to the Amadeus system (29 Oct 2026)
[4] Cathay Pacific: Personal data security
[5] Yonhap (Korean): Korean Air and Asiana, personal data leaked at reservation system operator (23 Oct 2026)
[6] Asia Business Daily (Korean): Korean Air and Asiana customer data leaked via contractor (23 Oct 2026)
[7] Reuters via StreetInsider: Cathay Pacific says Amadeus breach affected 53,000 bookings (30 Oct 2026)
[8] BleepingComputer: Japan Airlines suffers third-party data breach exposing passenger info
[9] heise online: Security vulnerability in flight booking system (13 Oct 2026)
[10] heise online (German): Reisebranche: BSI rät wegen Amadeus-Lücken zu Vorsicht (updated 15 Oct 2026)
[11] ISO/IEC 27001:2022 Information security management systems
[12] NIS2 Directive (EU) 2022/2555, Article 21 and Annex I
[13] DORA, Regulation (EU) 2022/2554, Articles 28 to 30
[14] The Mainichi (Kyodo): ANA says data on 37,800 customers leaked in hacking (30 Oct 2026)

Facts are from the airlines' own notices, Amadeus's own statement [16] and Amadeus statements quoted by named news reports, and those reports, as published by 2 Nov 2026. Amadeus has not published a root cause or a list of affected airlines. The control list and the framework mapping are Killswitch's own.

SOURCES

Sources (2/2)

[15] Malaysia Airlines: Cybersecurity Incident Involving Third-Party Technology Provider

[16] Amadeus: Amadeus statement (October 2026)

Facts are from the airlines' own notices, Amadeus's own statement [16] and Amadeus statements quoted by named news reports, and those reports, as published by 2 Nov 2026. Amadeus has not published a root cause or a list of affected airlines. The control list and the framework mapping are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Map your supplier and access controls, with the evidence

GRCOMPLIANCE

Keep your supplier register, access reviews and incident controls, owners and evidence in one place, mapped to ISO 27001, NIS2 and DORA.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.