November 20, 2026
Peach Aviation Limited

Unauthorized Access at Yumirulink Inc.: Apology and Notice Regarding the Leakage of Email Addresses and Other Personal Information

We have recently confirmed that "Cuenote FC," an email delivery service provided by Yumirulink Inc. that we utilize to send email newsletters and various notification emails to our customers, was subjected to unauthorized access by a third party, resulting in the leakage of customer personal information held by Peach.

Please note that critical information, such as credit card and passport details, is not included in the leaked data under any circumstances. Furthermore, there is no impact on reservations (including reservation changes) or flight operations.

We sincerely apologize for the considerable inconvenience and concern this incident has caused our valued customers and all parties involved.

Below is a summary of the facts confirmed to date, the affected information, and our ongoing response.

1. Overview
Date of Occurrence at Contractor: Sunday, October 18, 2026
Date Scope of Impact Confirmed: Friday, November 6, 2026
Affected Service: Yumirulink Inc. "Cuenote FC" (Email Delivery Service)
Incident Details: Server OS shutdown and full suspension of services following the detection of unauthorized third-party access to certain servers
Scope of Impact (Currently Suspended Services):

- Distribution of email newsletters (EDM)
- Automated notification emails (such as Peach Point expiration reminder emails)
- Refund Application Form used at airports and other locations

Status of Secondary Damage: At present, no unauthorized use of personal information or secondary damage related to this incident has been confirmed.

2. Status of Personal Information
Affected Customer Information: Name, date of birth, gender, address, phone number, email address, and itinerary details
Number of Affected Records: 8,997,106

3. Cause and Current Status
This incident occurred due to the detection of unauthorized third-party access within the server environment of "Cuenote FC," provided by our contractor, Yumirulink Inc.
As an emergency measure, the contractor shut down the servers, and all functions are currently suspended.
According to reports from Yumirulink Inc., it has been confirmed that this incident was not caused by ransomware; however, the company is currently investigating the intrusion route and the detailed scope of the impact.

4. Our Response
Notification to Affected Customers: Starting today, we will sequentially send an apology and notice to the registered email addresses of affected customers.
Fact-Finding and Thorough Investigation: We are working closely with the contractor to identify the exact scope of the impact.
Reporting to Relevant Authorities: We have already reported this incident to the Personal Information Protection Commission (PPC) and will continue to take appropriate action in accordance with the investigation results.

5. Impact on Services
Because the "Refund Application Form" used during irregular operations such as flight disruptions at airports is currently unavailable, we will handle any refund requests that may arise through alternative procedures.

6. Request to Customers
There is a possibility that suspicious emails, SMS messages, or phone calls impersonating our company may be sent to the email addresses or phone numbers affected by this incident.
Please exercise extreme caution and do not open any URLs or attachments contained in unsolicited or unfamiliar emails or SMS messages.

Should any new facts requiring disclosure come to light through ongoing investigations, we will promptly announce them on our official website and through other appropriate channels.