

【Important Notice】 Regarding Potential Leakage of Customer Information

Fujita Kanko INC. (Head Office: Bunkyo-ku, Tokyo; President & CEO: Shinsuke Yamashita; hereinafter “the Company”) previously confirmed that messages directing customers with reservations at facilities operated by the Company and at the Company’s group franchise facilities (hereinafter collectively “the Facilities”) to phishing sites (*1) had been sent. Following an investigation, it was found that information of certain customers who had made reservations at the Facilities may have been leaked through an external reservation management system (the “TEMAIRAZU Series” provided by Temairazu, Inc.; hereinafter “the reservation management system”). (*2)

*1 A “phishing site” is a fraudulent website impersonating a legitimate website and designed to obtain personal or financial information through deceptive means.

*2 Temairazu, Inc., notice dated September 29, 2026: [“Notice and Apology Regarding Suspicious Messages and Unauthorized Access to TEMAIRAZU”](#)

1. Affected Facilities

Facilities operated by the Company

HOTEL TAVINOS Hamamatsucho, HOTEL TAVINOS Asakusa, HOTEL TAVINOS Kyoto, Hotel Chinzanso Tokyo, Towada Hotel, Yugawara Onsen Chitose, and Hotel Yamanami

Company group facilities (franchises)

Koriyama Washington Hotel, Tachikawa Washington Hotel, Kisarazu Washington Hotel, Tsubame-Sanjo Washington Hotel, Takarazuka Washington Hotel, and Sasebo Washington Hotel

2. Incident Summary

On Tuesday, September 22, following an inquiry from a customer, the Company confirmed that notifications directing certain customers to phishing sites (*1) had been sent.

The subsequent investigation also confirmed that a cyberattack resulted in unauthorized access to the reservation management system and that personal information of certain customers may have been leaked.

As of the date of this notice, no financial losses have been reported.

The details of the incident remain under investigation. The Company will promptly provide an update if any new facts are confirmed.

3. Request to Customers

If you receive any suspicious communication, including an email or message, impersonating the reservation management system or an accommodation facility, please do not reply, access (click) any URL or link included in it, enter personal information such as credit card details, or make any payment or transfer of funds. To verify your reservation details, please contact the accommodation facility you booked or the online travel agent through its official contact channels.

If you have entered credit card information or other details on a suspicious website, please contact your credit card issuer promptly. Please note that the system involved in this incident does not handle or retain credit card information.

For inquiries regarding this matter, please contact the following:

Temairazu, Inc.

Department: Emergency Help Desk
Email: helpdesk@temairazu.com

The Company sincerely apologizes to its customers and all parties concerned for the considerable inconvenience and concern caused by this incident.

We ask that you continue to remain vigilant. Thank you for your understanding and cooperation.