

October 5, 2026

Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

Notice Regarding Leakage of Personal Information Due to Unauthorized Access by a Third Party to the Member Management System of Our Official Yakiniku King App

The Monogatari Corporation hereby announces that the member management system of the official Yakiniku King app operated by the Company (the “App”) was subject to unauthorized access by a third party, and that member information registered with the App was leaked. At this time, we have not confirmed any instances in which the leaked information has been publicly disclosed to an unspecified number of parties or used for unauthorized purposes.

We sincerely apologize for the considerable inconvenience and concern caused to customers using the App. The facts identified as of the date hereof and the status of our response are described below.

We are continuing to investigate this matter. If any new facts are identified as the investigation progresses, we will promptly provide further information.

1. Overview

On Friday, October 2, 2026, our company confirmed unauthorized access by a third party to the member management system of the official Yakiniku King app.

After detecting the unauthorized access, we blocked the unauthorized communications and implemented protective measures. However, on Saturday, October 3, 2026, we confirmed that member information had been leaked.

The App continues to provide services after the implementation of measures to protect against unauthorized access from external sources.

We have also implemented similar measures for the official apps of the Company's other brands, and no leakage of information or other related incidents have been identified in connection with those apps.

2. Personal Information Leaked

Of the 10,808,784 users registered with the official Yakiniku King App, information relating to 10,788,963 users was leaked.

The leaked information includes membership numbers, names (names registered with the App), email addresses, and telephone numbers.

No leakage has been identified with respect to the login passwords, dates of birth, gender information, postal codes, or store usage histories, including loyalty point balances, that are registered with the App. We do not retain payment information, such as credit card information.

3. Cause of the Information Leakage

We are currently conducting a detailed investigation into the cause of the incident and the circumstances that enabled the unauthorized access.

At present, we have confirmed that the information leakage resulted from unauthorized access by a third party.

October 5, 2026

4. Measures to Prevent Recurrence and Future Actions

With the cooperation of the system developer and other related companies, we will further strengthen our security measures and monitoring systems.

We are also taking necessary actions, including reporting the incident to the Personal Information Protection Commission and filing a damage report with the police.

5. Request to Customers

There is a risk that the personal information leaked in this incident may be misused for spoofing emails, phishing scams, or other fraudulent activities.

Customers are advised to exercise due caution regarding suspicious emails, SMS messages, telephone calls, and other communications, and not to open any links or attachments that they do not recognize.

We will never ask customers to provide passwords, credit card information, or other similar information. We once again ask customers to exercise due caution.

6. Impact on Financial Results

The impact of this incident on the financial results of our group is currently under review.

We will promptly disclose any matters that require disclosure as they arise.