August 28, 2026

Company name: Treasure Factory Co., Ltd.
Name of representative: Eigo Nosaka, President & CEO
(Securities code: 3093; Tokyo Stock Exchange, Prime Market)
Inquiries: Takaaki Kanesaka, Executive Officer, General Manager of Corporate Planning Office
(Telephone: +81-3-3880-8822)

Notice Regarding Personal Information Leakage Due to Unauthorized Access at Our Consolidated Subsidiary

Treasure Factory Co., Ltd. (the "Company") has confirmed that a third party gained unauthorized access to the e-commerce site operated by Kindal Co., Ltd. (hereinafter referred to as the "Subsidiary"), a consolidated subsidiary of the Company, resulting in the leakage of its customers' personal information. The Company hereby provides notice of the details as follows.
The Company sincerely apologizes to its customers and all other parties concerned for the significant concern and inconvenience this incident has caused.

1. Overview of the Incident

A third party gained unauthorized access to a staff account on the e-commerce platform used to operate the e-commerce site run by the Subsidiary.
On August 24, 2026, while exporting order information in the course of regular business operations, the Subsidiary discovered that the e-mail address registered to the staff account had been changed to one not used by the Subsidiary. The Subsidiary therefore requested that the company operating the e-commerce platform conduct an investigation.
As a result of that investigation, it was confirmed that a third party had gained unauthorized access to the staff account on August 22, 2026, that the account's registered e-mail address was subsequently changed on August 23, and that on the same day, a bulk export of customer information was executed on two occasions.

2. Personal Information Leaked

As of the current time, 136,464 individuals have been confirmed as affected, of whom 109,311 had their address information included.
The information that may have been affected is as follows:
Customer ID, name, address, phone number, date of birth, e-mail address, e-mail newsletter subscription status, total number of orders, total purchase amount, customer tag information managed on the e-commerce platform, and reward points history (current balance, expired points, and cumulative points)

※ The specific items of information affected vary by customer.

※ The Company has confirmed that the data exported on this occasion did not include credit card information or the login passwords for the e-commerce site.

※ At this time, no fraudulent use of personal information or other concrete secondary damage resulting from this incident has been confirmed.

3. Cause

An internal investigation confirmed that a phishing e-mail impersonating the company operating the e-commerce platform had been sent to the employee who used the staff account subject to the unauthorized access, and that the account's authentication credentials had been entered on a linked page referenced in that e-mail.

An investigation of the logs on the relevant PC found that the first instance of unauthorized access identified in this incident occurred immediately after the authentication credentials were entered. Based on this, the Group has determined that the cause of this unauthorized access was that a third party obtained the staff account's authentication credentials through this phishing e-mail.

In addition, two-factor authentication had not been configured for the staff account in question, such that it was possible to log in using only an e-mail address and password, and the password that had been set was also not sufficiently strong.

The Company recognizes that these deficiencies in credential management were also a contributing factor to the failure to prevent the unauthorized access.

4. Response Status

Upon discovering this incident, the Subsidiary immediately implemented the following measures:

- Deleting the staff account that was subject to unauthorized access
- Checking all other staff accounts for any suspicious access or operations
- Making two-factor authentication mandatory for all staff accounts on the e-commerce platform
- Requesting that the company operating the e-commerce platform conduct a further investigation into whether any additional operations were carried out from the account after the unauthorized export of customer information

In addition, the Subsidiary reported this incident to the Personal Information Protection Commission on August 27, 2026.

5. Contact for Inquiries

Affected customers will be notified individually, in due course, of the details of this incident and related points of caution. The Company is also currently preparing to establish a dedicated contact point for inquiries regarding this incident. Once it is in place, the Company will promptly announce it on the websites of both Treasure Factory Co., Ltd. and Kindal Co., Ltd.

6. Future Response and Measures to Prevent Recurrence

Since discovering this incident, the Subsidiary has made two-factor authentication mandatory for all staff accounts and is conducting a review of the status of its account and access rights management.

In light of the cause identified in this incident, the Subsidiary will also strengthen its countermeasures against phishing e-mails, thoroughly carry out information security education and anti-phishing training

for employees, review rights to access customer information and to perform bulk exports, and enhance its monitoring and escalation systems in order to detect suspicious logins, changes to important account information, large-volume data exports, and similar activity at an early stage.
Rather than treating this incident as an issue specific to the Subsidiary alone, the Company will also review, across the Group, the status of two-factor authentication settings, account and access rights management, rights to export information, and security monitoring systems for the systems and cloud services used by the Group, and will strengthen anti-phishing measures and information security education Group-wide in order to prevent recurrence.

7. Impact on Financial Results

The Company is currently assessing the impact of this incident on the Group's consolidated financial results.
Should it become clear that this incident will have a material impact on financial results, or should any other matter requiring disclosure arise, the Company will promptly announce it.