October 23, 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 to the Company's System

Treasure Factory Co., Ltd. (the "Company") has confirmed that a third party gained unauthorized access to the request management system used by the Company for its home-visit purchase and Treasure Factory Moving & Removal services (hereinafter referred to as the "Request Management System"), and that part of the customer information and other information held by the Company was illicitly obtained by an outside party. The Company hereby provides notice of the details as follows. The Company sincerely apologizes to its customers, shareholders, investors, and all other stakeholders for the significant concern and inconvenience this incident has caused.

1. Overview of the Incident

On October 20, 2026, an investigation of the access logs of the Request Management System conducted by the Company confirmed that, from the early hours through the morning of the same day, a third party had gained unauthorized access to the Company's system by exploiting a vulnerability, and that customer information and other information had been illicitly obtained.
At 10:30 a.m. on the same day, the Company suspended external access to the Request Management System, and at 11:05 a.m., it suspended the acceptance of requests through the application forms for home-visit purchases, moving services, and other services.

2. Scope of Impact Confirmed to Date

To date, the Company has confirmed that the following information was illicitly obtained.
Customer information entrusted to the Company at its stores and that registered through the Company's app are stored in systems separate from the Request Management System that was subject to the unauthorized access, and are not included in the information illicitly obtained in this incident. In addition, at this time, no fraudulent use of personal information or other concrete secondary damage resulting from this incident has been confirmed.

(1) Customer information: 746,277 records

Compromised information: E-mail addresses

Of these, 11 records also include names and addresses.

The Company has confirmed that the customer information illicitly obtained in this incident did

not include credit card numbers, security codes, or any other payment-related information.

(2) Information on business partners, employees, and others: 750 records
Compromised information: Names and e-mail addresses

(3) Information on devices used by business partners, employees, and others: 1,000 records
Compromised information: Names and device identification information

3. Cause

Based on the investigation to date, the Company believes that the cause was the exploitation by a third party of a vulnerability related to access to the database. The Company will continue to investigate the detailed cause and scope of impact in cooperation with external security specialists.
The Company has confirmed that the unauthorized access in this incident did not exploit the recently disclosed vulnerability related to PHP and is unrelated to that vulnerability.

4. Response to Date and Measures to Prevent Recurrence

After confirming the unauthorized access, the Company suspended external access to the Request Management System and has taken measures such as changing the passwords of related accounts.
At the same time, the Company is addressing the vulnerability exploited in this incident, strengthening the security of the login function, and enhancing the monitoring of suspicious access, among other measures.
The Company plans to resume the system and the application forms around October 28, 2026, after implementing and confirming the necessary safety measures.
Following the personal information leakage due to unauthorized access that occurred in August 2026 at Kindal Co., Ltd., a consolidated subsidiary of the Company, the Company and its group companies (collectively, the “Group”) have been reviewing and strengthening two-factor authentication settings, account and access rights management, data export permissions, security monitoring systems, and other matters across the entire Group.
While the previous incident was caused by a third party obtaining a staff account's authentication credentials through phishing, this incident involved the exploitation of a vulnerability related to access to the database, and the cause and intrusion route differ between the two incidents. Nevertheless, the Company takes very seriously the fact that multiple information security incidents have occurred within the Group in a short period of time. In addition to the strengthening of authentication management, access rights management, monitoring systems, and other measures that have been underway, the Company will once again review vulnerability management for externally accessible systems, vulnerability assessments, protection using a web application firewall (WAF) and other means, and security measures for applications and databases, and will work to further strengthen the information security management system of the entire Group.

5. Reports to Relevant Authorities and Other Matters

The Company is in the process of reporting this incident to the Personal Information Protection Commission and consulting with and reporting to the police and other relevant authorities. The Company will provide the necessary information individually to affected customers and others, and is also preparing to establish a dedicated contact point for inquiries regarding this incident. Once the

contact point has been established, the Company will promptly announce the details on its website.

6. Impact on Financial Results

The Company is currently assessing the potential 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.