October 13, 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 the Investigation Results and Measures to Prevent Recurrence Concerning the Personal Information Leakage Due to Unauthorized Access at Our Consolidated Subsidiary (Third Report)

Further to the Company's announcements on August 28 and September 2, 2026 regarding the leakage of personal information due to unauthorized access at Kindal Co., Ltd. (hereinafter referred to as the "Subsidiary"), a consolidated subsidiary of Treasure Factory Co., Ltd. (the "Company"), the Subsidiary has completed its investigation. The Company hereby announces the investigation results, measures to prevent recurrence, and other related matters as detailed below. The Company once again sincerely apologizes to its customers and all other parties concerned for the significant concern and inconvenience this incident has caused.

1. Investigation Results

The Subsidiary conducted its investigation by cross-checking the phishing e-mail, the PC logs of the employee who received the phishing e-mail, and the results of the investigation of access and operation histories conducted by the company operating the e-commerce platform, and has identified the unauthorized access route and how the information was exfiltrated. The results of the investigation are as follows:

- The number of individuals affected by the personal information leakage has been finalized at 136,464 (including 109,311 whose address information was included). The items of information leaked are unchanged from those announced on August 28, 2026, and did not include credit card information or the login passwords for the e-commerce site.
- As announced in the first report, the cause of the unauthorized access was the theft of the staff account's authentication credentials through a phishing e-mail. The Subsidiary recognizes several management issues: the lack of two-factor authentication, authentication methods and account protection that were inadequate against phishing attacks, shortcomings in the design of bulk export permissions for customer information, and an insufficient monitoring system for the early detection of important operations.
- At this time, no fraudulent use of personal information or other concrete secondary damage resulting from this incident has been confirmed.
- The Subsidiary submitted its final report to the Personal Information Protection Commission on

October 6, 2026. The Subsidiary has also consulted the police and is in the process of filing a formal incident report.

2. Measures to Prevent Recurrence

(1) Measures at the Subsidiary

The Subsidiary has introduced two-factor authentication using passkeys, a phishing-resistant method, for all staff accounts, and has also conducted an inventory of accounts, restricted bulk export permissions for customer information, and reviewed its procedures for confirming and internally escalating important operations, among other measures. In addition, the Subsidiary is progressively developing an information security manual, providing education including anti-phishing training, conducting periodic reviews of access rights, and establishing a monitoring system.

(2) Measures across the Group

In response to this incident, the Group has reviewed its cybersecurity measures as follows:

- Developed information security guidelines applicable to all Group companies (stipulating, among other things, mandatory multi-factor authentication for external tools that hold personal information and other data, restrictions on bulk export permissions for customer data, and the implementation of training against targeted attack e-mails), and appointed an information security officer at each Group company
- Revised the operating policy of the Cybersecurity Incident Response Team (CSIRT) and established operational and reporting systems covering all Group companies
- Established an Information Security Liaison Council comprising the information security officers of all Group companies, and put in place a framework for continuously strengthening the Group's cybersecurity through regular meetings of the Council
- Implemented periodic inventories of the account management, access rights, and authentication status of external tools used by all Group companies (the first inventory was conducted in September 2026, and remediation of items assessed as high risk is underway)

3. Contact for Inquiries

For the time being, inquiries regarding this incident are being accepted at the following desk:

Kindal Co., Ltd. Dedicated Inquiry Desk

Phone number: 0120-721-616 (Toll-free; available only within Japan)

Hours: 9:00 a.m. to 6:00 p.m. on weekdays (Japan Standard Time)

4. Impact on Financial Results

Although costs related to this incident, such as those for operating the dedicated inquiry desk, have been incurred, the impact on the Group's consolidated financial results is immaterial, and there is no change to the consolidated earnings forecasts for the fiscal year ending February 2027. Should any matter requiring disclosure arise in the future, the Company will promptly announce it.