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.

November 9, 2026

To Whom It May Concern

Company name:Nitori Holdings Co., Ltd.
Listing: Tokyo, Sapporo
Securities code: 9843
Representative: Toshiyuki Shirai Representative Director & Chief Operating Officer (COO)
Inquiries: Teruo Yoshioka Manager, Public Relations Division
Telephone: +81-3-6741-1213

Apology and Notice Regarding the Potential Leakage of Personal Information Resulting from Unauthorized Access to Our Systems

We sincerely appreciate your continued patronage of the Nitori Group.

On November 6, 2026, Nitori Holdings Co., Ltd. (the “Company”) confirmed that a third party had gained unauthorized access to systems managed by the Company. Based on the investigation conducted to date, it has been determined that up to 37.62 million records of personal information stored on the Company’s servers may have been disclosed to an external party. Login passwords and credit card information are not included in the information that may have been disclosed.

The information potentially affected includes personal membership information and information relating to customers who purchased products from the Nitori Group, including membership numbers, names, names in Japanese phonetic characters, email addresses, addresses, telephone numbers, dates of birth, and gender; corporate membership information, including membership numbers, company names, department names, names of company representatives, company addresses and telephone numbers, and the names, email addresses, and telephone numbers of contact persons; and order information relating to customers who purchased the Company’s products through official Nitori stores on e-commerce marketplaces. The specific combination of information potentially affected varies by customer.

We sincerely and deeply apologize for the considerable inconvenience and concern caused to our customers, business partners, and all other stakeholders. The information currently known and the measures being taken by the Company are set forth below.

1. Overview of the Incident

On November 6, 2026, the Company identified unauthorized access to systems under its management. The Company immediately blocked the unauthorized access and, in cooperation with external cybersecurity experts, commenced an investigation into the scope and impact of the incident.

The subsequent investigation has identified the possibility that unauthorized access by a third party may also have occurred prior to November 6. The Company is continuing to investigate the detailed circumstances surrounding the incident.

Access by the threat actor has been blocked. The Company continues to analyze system logs and verify relevant data to determine the scope and number of affected records. Accordingly, the information currently available may change as the investigation progresses.

2. Timeline of the Unauthorized Access

Date	Event Identified	Status
Mid to late October	Possible access by a third party	Through system log analysis and other investigations conducted after the incident was identified on November 6, the Company confirmed the possibility that access by a third party may also have occurred before that date. The details remain under investigation.
Friday, November 6	Identification of unauthorized access and initial response	Upon identifying the unauthorized access, the Company blocked the access and, in cooperation with external cybersecurity experts, commenced an investigation into the cause, intrusion route, and scope of impact.

3. Personal Information That May Have Been Accessed by an External Party

Maximum number of records potentially affected: 37.62 million

The categories of information potentially affected are listed below. The specific combination of information varies by customer.

- **Individual members and customers who purchased products from the Nitori Group:** Membership number, name, name in Japanese phonetic characters, email address, address, telephone number, date of birth, and gender
- **Corporate members:** Membership number, company name, department name, name of the company representative, company address and telephone number, and the name, email address, and telephone number of the contact person
- **Relevant services:** Order data relating to purchases of the Company's products through Nitori Net and official Nitori stores on e-commerce marketplaces

Credit card information and login passwords are not included in the information affected by this incident.

4. Current Response Status

- The Company continues to block access by the threat actor. Measures have been implemented to address the relevant vulnerabilities, and the enhancement of the monitoring framework has been completed.
- In cooperation with external cybersecurity experts, the Company is continuing to investigate the cause of the incident, the intrusion route, the scope of impact, and whether any secondary damage has occurred.

5. Notification to Affected Customers

The Company will contact affected customers individually by email or postal mail on a sequential basis.

6. Important Notice to Customers

The personal information that may have been disclosed could potentially be misused for fraudulent emails, phishing scams, suspicious telephone calls, or other forms of impersonation.

Please exercise caution regarding communications purporting to be from the Company, delivery service providers, e-commerce marketplaces, or other related parties. Please do not open links or attachments contained in communications that you do not recognize or were not expecting.

The Company will never ask customers by email or telephone to provide passwords, credit card numbers, personal identification numbers, or similar confidential information.

If you receive a suspicious communication, please do not reply to or contact the details provided in that communication. Instead, please contact the dedicated inquiry desk to be posted on the Company's official website.

7. Future Measures

The Company takes this incident extremely seriously and, with the continued assistance of external cybersecurity experts, will proceed with verifying the facts and determining the cause of the incident.

Based on the results of the investigation, the Company will review its access controls, authentication and authorization management, monitoring framework, and other relevant security measures, and will implement measures to prevent a recurrence.

If any additional matters requiring public disclosure are identified, the Company will provide an update promptly.

8. Reports to Relevant Authorities

The Company is reporting and consulting on this incident with the Personal Information Protection Commission of Japan, the police, and other relevant authorities.

The Company will appropriately implement all necessary measures in accordance with the guidance and advice provided by the relevant authorities.

We once again extend our deepest apologies to our customers and all other stakeholders for the inconvenience and concern caused by this incident.

Inquiries from Customers and Other Stakeholders

Customer Service Department
Nitori Holdings Co., Ltd.

Telephone: 0120-209-993
Hours: 10:00 a.m. to 8:00 p.m., including weekdays, weekends, and public holidays

Inquiry form: https://www.nitori-net.jp/ec/input-inquiry?inquiryRecordCode=04000000

Media Inquiries

Public Relations Department
Nitori Holdings Co., Ltd.

Email: koho@nitori.jp
Telephone: +81-3-6741-1213
Hours: 10:00 a.m. to 6:00 p.m. on weekdays

9. Impact on Financial Results

The impact on our financial results is currently under review, taking into account the measures to be implemented going forward. Based on the information available at this time, however, the impact on our consolidated financial results is expected to be limited**.**Should any matters requiring disclosure arise in the future, we will promptly make an announcement.