

October 9, 2026

Company name: BOOKOFF GROUP HOLDINGS LIMITED
Name of representative: Yasutaka Horiuchi
President and CEO
(Securities code: 9278; TSE Prime Market)
Inquiries: Takashi Hasegawa
Executive Officer, General Manager of Group
Strategic Planning Department
(Telephone: +81-42-750-8588)

Apology and Notice Regarding Personal Information Leakage Due to Unauthorized Access

BOOKOFF GROUP HOLDINGS LIMITED (the “Company”) hereby announces that it has confirmed that a third party gained unauthorized access to a system used by one of the Company’s subsidiaries to manage member information, and that member information was leaked outside the Company.

As of the date hereof, the Company has not confirmed that the leaked information has been publicly disclosed or misused by any third party.

The Company sincerely apologizes for the considerable concern and inconvenience caused to its customers.

The following provides an overview of the incident and the measures taken by the Company as of the date hereof. The Company will continue to conduct a detailed investigation and will promptly make a further announcement if any new facts are identified.

1. Overview of the Incident

On Tuesday, October 6, 2026, the Company confirmed that a third party had gained unauthorized access to the member management system of one of its subsidiaries. As a result of its investigation, the Company determined that member information managed in the system had been obtained from outside the Company.

2. Scope of Impact

Number of Member Data Records That May Have Been Leaked

Up to approximately 6.43 million records (*1)

Information That May Have Been Leaked

Names, dates of birth, gender, email addresses, telephone numbers, postal codes and addresses, password hash values (*2), point card numbers, and membership numbers

Payment information, including credit card information, is not included, as such information is not stored in the relevant system.

As of the date hereof, the Company has not confirmed any alteration of member information. The Company is continuing to carefully examine the actual number of affected individuals and the information that may have been leaked, and will make a further announcement once the details have been determined.

*1 This figure represents the number of membership numbers that may have been leaked and does not represent the actual number of affected individuals.

*2 Password hash values are encrypted and cannot be read in their current form.

3. Request to Customers

If information that may have been obtained in connection with this incident is misused, members may receive emails, SMS messages, telephone calls or other communications impersonating the Company Group or related parties. The Company requests that members take the following precautions:

- Exercise caution with suspicious emails, SMS messages and telephone calls impersonating the Company Group or related parties.
- Do not open URLs or attachments contained in unfamiliar communications, and do not enter any personal information or authentication credentials.
- The Company Group will not request passwords, authentication codes, credit card information, bank account information or similar information by email, SMS message, telephone call or any other means.
- If any suspicious communication or unauthorized use is identified, please contact the customer inquiry desk set forth below.

4. The Company's Response and Future Measures

Following confirmation of the unauthorized access, the Company blocked communications from the source of the attack, remedied the vulnerability and blocked external access to the affected system. The Company has completed containment of the route currently identified as having been used to obtain the information without authorization and continues to monitor the situation.

In addition, the Company is conducting an emergency comprehensive inspection of all systems and is implementing additional security measures and permanent measures to prevent recurrence from both network and application perspectives.

The Company is also taking the necessary actions, including submitting a report to the Personal Information Protection Commission. Based on the results of the investigation, the Company will contact the affected customers individually in due course.

5. Contact Information Regarding This Incident

Customer Inquiry Desk

Inquiry form: <https://www.bookoffgroup.co.jp/contact-us/contact-us-261009/>

Customer service telephone number: 0570-01-2902 (Navi Dial)

Business hours: 10:00 a.m. to 6:30 p.m.

Shareholder and Investor Inquiry Desk

Inquiry form: <https://www.bookoffgroup.co.jp/contact-us/top/contact-us-01/>

Media Inquiry Desk

Inquiry form: <https://www.bookoffgroup.co.jp/contact-us/top/contact-us-02/>

The Company takes this incident very seriously and will continue to investigate the facts and the scope of impact, review its security framework and implement measures to prevent recurrence. If any new facts requiring public disclosure are identified, the Company will promptly make a further announcement.