(Notice)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 6, 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 (Third Report)

With respect to the "Apology and Notice Regarding Personal Information Leakage Due to Unauthorized Access (First Report)" announced on October 9, 2026, the "Apology and Notice Regarding Personal Information Leakage Due to Unauthorized Access (Second Report)" announced on October 13, 2026 and partially corrected on October 16, 2026, and the "Notice Regarding the Addition of a Web Inquiry Function and the Opening of a Dedicated Toll-Free Number for the Personal Information Leakage Due to Unauthorized Access" posted on its website on October 23, 2026, BOOKOFF GROUP HOLDINGS LIMITED (the "Company") hereby provides this third report on the results of its subsequent investigation, the status of its response to customers, and measures to prevent recurrence.

As of the date hereof, the Company has not confirmed that the leaked member information has been made public, that points have been used fraudulently, or that customer member information has been altered. There has also been no change to the scope of impact (affected services, number of affected individuals, and information that may have been leaked) disclosed in the second report. All systems of the Group are operating normally, and the incident has not affected business continuity.

The Company once again sincerely apologizes for the considerable concern and inconvenience caused to its customers and other stakeholders.

1. Background and Current Status of the Incident

On October 6, 2026, BOOKOFF CORPORATION LIMITED ("BOOKOFF CORPORATION"), a consolidated subsidiary of the Company, confirmed unauthorized access by a third party to its member management system. The investigation confirmed that member information managed in the system was obtained externally between October 4 and October 6, 2026.

Immediately after discovering the incident, BOOKOFF CORPORATION blocked communications from the source of the attack and the route used for the unauthorized access. No new unauthorized acquisition of member information has been confirmed since the blocking was completed.

Subsequently, the investigation into the cause, conducted with the assistance of external specialists, revealed that a third party had exploited an access control issue in certain functions of the system handling member information to obtain such information. The investigation into this incident has identified the route and cause of the unauthorized access.

The Company has already submitted the required information to the Personal Information Protection Commission in a preliminary report and plans to submit a final report in early December. The Company will also continue to cooperate with the police investigation, including by submitting necessary materials upon request.

The Group's stores, official online store, official app, and other services are currently available as usual.

Services Covered by the Incident (unchanged from the second report as corrected on October 16, 2026)

Coverage	System	Company Group Services	Business Segment
Covered	BOOKOFF member management system	BOOKOFF SUPER BAZAAR BOOKOFF PLUS BOOKOFF BOOKOFF Official Online Store Aso-viva BOOKOFF FASHION BINGO B・SPORTS B・STYLE	BOOKOFF operations in Japan
		Rehello by BOOKOFF (stores)	Premium Services Business
Not covered	Managed in systems separate from the above	hugall aidect Rehello by BOOKOFF (e-commerce site)	Premium Services Business
		Japan TCG Center Booklog Aoyama Book Center BOOKOFF Clean-up Service	Other Business

2. Scope of Impact (unchanged from the second report as corrected on October 16, 2026)

(1) Number of Affected Member Data Records and Individuals

Item	Confirmed Information
Number of leaked member data records	6,427,735 membership-number-based records
Number of affected individuals	6,383,279 individuals (6,170,908 active members and 212,371 former members)

The number of leaked member data records is the number of membership numbers for which system logs confirmed that member information was transmitted externally. The number of affected individuals counts multiple member data records registered under the same email address as one individual. This difference in counting methodology accounts for the difference between the number of member data records and the number of affected individuals.

The affected members are BOOKOFF Official App members, BOOKOFF Official Online Store members, and BOOKOFF Web members. Customers who use only a membership card and have not registered through the app or the web are not included.

(2) Information That May Have Been Leaked

Payment information, including credit card information, and bank account information are not included because they are not managed in the member management system affected by this incident. In addition, images of identity verification documents presented for in-store purchases from customers are not saved or retained.

Images of identity verification documents submitted for home-delivery purchase services through the BOOKOFF Official Online Store are managed in a system separate from the member management system affected by this incident and are therefore not included. As of the date hereof, no alteration of member information or fraudulent use of points has been confirmed.

Category of Information	Covered / Not Covered
Information registered by BOOKOFF Official App members, BOOKOFF Official Online Store members, or BOOKOFF Web members: name, date of birth, gender, occupation, nickname, email address, telephone number, postal code and address registered as member information, password hash value (*1), point card number, and membership number	Covered
Address entered for in-store purchases from customers and text information read from a driver's license or other identity verification document	Not covered

Delivery destination information specified when ordering products that differs from the registered member address, including name, address, and telephone number	Not covered
Pickup address specified for home-delivery purchase services that differs from the registered member address, and images of identity verification documents	Not covered

*1 A password hash value is information generated by converting a password using a prescribed method; the original password cannot be read directly from the hash value.

3. Status of the Response to Affected Members

The Company began sequentially sending individual emails to members affected by this incident on October 15, 2026, and completed sending emails to all email addresses to which it had confirmed emails could be sent on October 22, 2026. In addition, from October 26 to October 29, 2026, the Company individually notified affected members through notifications in the BOOKOFF Official App.

The Company has also added a web inquiry function to the BOOKOFF member website that allows customers to check for themselves whether they are affected by this incident. In addition, a dedicated toll-free number for this incident has been available since October 22, 2026 to respond to inquiries.

The Company will continue to respond sincerely to customers' opinions and inquiries and strive to restore trust through ongoing dialogue with affected members.

4. Measures to Prevent Recurrence

The Group takes this incident very seriously and is implementing measures to prevent recurrence in stages, based on the results of the investigation into the cause of this incident and advice from external specialists. In addition to addressing the direct cause of this incident, the Group will strengthen its security management framework across the entire Group.

(1) Measures Implemented

• Blocking the Route Used for Unauthorized Access and Strengthening Access Controls

The Group blocked the route used for unauthorized access in this incident, inspected externally accessible systems and functions, reviewed the scope of external accessibility, and strengthened access controls.

• Strengthening Security Measures for the Affected System

The Group implemented measures to address the direct factors that led to the unauthorized access in this incident and strengthened security measures by reviewing system authentication and authorization, communications controls, and other measures. In addition, the Group conducted a comprehensive inspection of the affected system and is continuing to remediate the issues identified.

• Strengthening Monitoring for Unauthorized Access

The Group strengthened monitoring of access to the affected system and established a framework for the early detection of unusual access or behavior.

(2) Measures in Progress

• Verifying Security with the Expertise of External Specialists

The Group is addressing vulnerabilities throughout the affected system and verifying its security, drawing on the expertise of external specialists. In addition, to verify the effectiveness of the measures objectively and on an ongoing basis, the Group is strengthening its verification framework, including third-party assessments.

• Strengthening Security Inspections of the Group's Systems

The Group is reassessing security risks in its systems, focusing on systems accessible from the internet and functions for external connections, and is implementing necessary corrective measures in stages.

• Reviewing the Incident Detection and Response Framework

To identify security anomalies at an earlier stage and facilitate appropriate decisions and responses, the Group is reviewing its processes for monitoring, reporting, escalation, and initial response.

(3) Measures to Be Implemented

• Strengthening Continuous Monitoring and Detection

In light of the increasing sophistication and complexity of cyberattacks, the Group will strengthen its framework for continuous security monitoring and detection.

• Strengthening Security Management in System Development and Operation

The Group will review security standards at each stage of system planning, design, development, and operation, and thoroughly conduct security checks of functions for external connections, including authentication, authorization, and access controls. The Group will also strengthen its arrangements for conducting vulnerability assessments, third-party assessments, and other checks on an ongoing basis.

• Strengthening Security Governance across the Group

The Group will strengthen its security management framework across the entire Group, including the ongoing identification of security risks, management of critical systems, incident response arrangements, and education and training.

Under the ongoing supervision of management and the Board of Directors, the Group will regularly review the implementation status and effectiveness of these measures to prevent recurrence, drawing on the expertise of external specialists, and will revise and improve them as necessary. The Company will refrain from disclosing specific system configurations, security products, settings, and other technical details because such information could be exploited for further unauthorized access or other malicious activities.

5. Request to Members (to Prevent Secondary Damage)

To prevent secondary damage arising from the unauthorized use of information or other activities related to this incident, the Company asks affected members to continue to observe the following precautions. The Company apologizes for the inconvenience this may cause.

- Please change the passwords used for the BOOKOFF Official Online Store and the BOOKOFF Official App. If the same or a similar password is used for any other service, please change it to a different password for that service as well.
  The notification email sent by the Company will not contain a link directing recipients to a password change page. To change a password, please access the official app or official website directly and complete the procedure.
- Exercise caution with suspicious emails, SMS messages, and telephone calls impersonating the Group or related parties.
- Do not open URLs or attachments in unfamiliar communications, and do not enter personal information or authentication credentials.
- The Group will not request passwords, credit card information, bank account information, or similar information by email, SMS message, telephone call, or any other means.
- If you identify any suspicious communication or unfamiliar use, please contact the inquiry desk below.

6. Response in the Event of Secondary Damage

As of the date hereof, no secondary damage arising from this incident, including the unauthorized use of customer information, has been confirmed. The Group will continue additional investigations and monitoring and work to prevent secondary damage.

If you suffer specific damage arising from this incident, or suspect that such damage has occurred, please contact the Customer Inquiry Desk below. If secondary damage arising from this incident is confirmed, the Group will verify the facts on an individual basis and respond appropriately. If it is confirmed that points have been used fraudulently as a result of this incident, the Group will fully restore the affected points.

7. Impact on the Group’s Financial Results

Expenses related to the investigation of this incident, notifications to customers, operation of the inquiry desk, and strengthening of security measures are expected to be recorded from the second quarter of the fiscal year ending May 31, 2027 onward. The Group’s stores and official online store have continued to operate as usual since the discovery of this incident. As of the date hereof, the impact of this incident on both net sales and expenses is limited.

In light of the above, there is no change to the consolidated financial forecasts for the fiscal year ending May 31, 2027 announced on July 13, 2026. If any matter requiring disclosure, including a revision to the financial forecasts, arises, the Company will promptly make an announcement.

8. Contact Information Regarding This Incident

Customer Inquiry Desk

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

Customer service telephone number: 0120-300-663 (toll-free)
Business hours: 10:00 a.m. to 6:30 p.m. (open every day)

* Frequently asked questions regarding this incident are available at the following URL:
https://ssl4.eir-parts.net/doc/9278/ir_material10/287328/00.pdf

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 give the highest priority to providing information and support to customers while reviewing the Group's security framework and implementing measures to prevent recurrence. If any new facts requiring public disclosure are identified, the Company will promptly make an announcement.