News Release Dated March 17, 2025

Company: AOKI Holdings Inc.
Representative: Haruo Tamura, President
Stock code: 8214, TSE Prime
Contact: Satoshi Eguchi,
General Manager of IR Office
Tel: +81-45-941-1388

Unauthorized Access and Possibility of Stolen Personal Information at a Consolidated Subsidiary (Third Report)

Unauthorized access at a server of KAIKATSU FRONTIER Inc., a subsidiary of AOKI Holdings Inc., may have resulted in a data breach involving some customer personal information. Information about this incident was reported in releases dated January 21 and January 28, 2025. The results of the investigation by an external security specialist and AOKI Holdings and measures to prevent this type of incident from happening again are as follows.

Since this cyberattack was discovered, the investigation has not discovered at this time any stolen personal information or any secondary damage involving the potential data breach of this information. AOKI Holdings sincerely apologizes to customers and others for the concerns and problems caused by the cyberattack.

Responses to this incident

In the evening of Saturday, January 18, 2025, unauthorized access was detected on a server used by KAIKATSU FRONTIER. The server was immediately isolated from external networks and other necessary actions were taken. An investigation was conducted with the assistance of an external security specialist to determine the severity of the effects of this cyberattack. The investigation confirmed unauthorized access to the system used for managing the accounts of members, which indicates that some customer information may have been stolen.

Following the discovery of this problem, AOKI Holdings immediately established a cyberattack response headquarters and started activities to determine the severity and cause of the attack. In addition, AOKI Holdings began working with the police and sent reports to the Personal Information Protection Commission.

AOKI Holdings has taken the following actions since the discovery of the cyberattack.

- Monday, January 20, 2025 Established cyberattack response headquarters and restricted use of the member app service
- Tuesday, January 21, 2025 First report to the Personal Information Protection Commission, first public announcement
- Tuesday, January 21, 2025 to Friday, February 14, 2025
  Investigations by an external security specialist and by AOKI Holdings
- Tuesday, January 28, 2025 Additional report to the Personal Information Protection Commission, second public announcement
- Friday, February 14, 2025 Received results of the investigation by the external security specialist
- Wednesday, February 19, 2025 to Friday, February 28, 2025
  Began the gradual resumption of member app service operations
- Thursday, March 13, 2025 Final report to the Personal Information Protection Commission
- Monday, March 17, 2025 Third public announcement

Information determined by the investigation

- The reason the server was vulnerable to unauthorized access and programs impacted by this attack
- The types and volume of information that may have been stolen

Potentially affected subjects and stolen personal information

Subjects: KAIKATSU CLUB members (Some of the individuals who visited stores between October 1, 2015 and January 20, 2025)

KAIKATSU CLUB provisional members (Some of the individuals who became members between March 25, 2019 and January 20, 2025)

FiT24 members and FiT24 Indoor Golf members (Some of the individuals who became members between October 30, 2018 and April 1, 2023)

Personal information: Full name / full name in Katakana, gender, postal code, address, phone number, birth date, membership number, membership type, membership status, current points balance and expiration date, shop code, the most recent transaction date and time, barcode, push notification request, coupon message

Personal information records: 7,290,087

* Provisional members are individuals who have not yet completed their membership registrations at the store.
* The personal information that may have been stolen does not include driver's licenses or other items used for personal identification, credit card data, e-mail addresses, or passwords for membership applications provided during membership registration.

Notification of individuals potentially affected

KAIKATSU FRONTIER notified individuals potentially affected by this cyberattack by using e-mail, postal mail and other methods between Wednesday, January 29 and Thursday, March 13, 2025.

Furthermore, KAIKATSU FRONTIER assumes that this release and the announcement as of March 17, 2025 by KAIKATSU FRONTIER serve as notification for individuals who could not be contacted by using any other method.

Preventive measures

The following actions have been taken based on the results of the investigation.

- The software that was affected by the unauthorized access has been revised.
- New security software and security patches have been installed.
- More rigorous oversight to prevent unauthorized access to the website and block access when malicious activity is detected.

In addition to these actions, servers and programs that were not affected by the unauthorized access were checked to be certain there are no negative effects. The password policy has been upgraded and more cybersecurity measures have been implemented for protection against cyberattacks, including surveillance and a multi-layered defense.

AOKI Holdings and KAIKATSU FRONTIER will continue working with external security specialists to build an even more powerful cybersecurity framework and strengthen surveillance system to prevent this type of incident from happening again.

Impact on results of operations

There are no revisions to the earnings forecast for this matter at this time. An announcement will be made promptly if there is any information that requires disclosure.

Media contact for more information about this subject

AOKI Holdings Inc. PR Office
Tel: +81-45-942-0408
Operating hours: 9:30 to 18:30 (Except Saturdays, Sundays and public holidays)