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.

October 22, 2026

Press Release

3-1-3, Uchihiranomachi, Chuo-ku
Osaka, 540-0037, Japan
Capcom Co., Ltd.
Haruhiro Tsujimoto, President and COO
(Code No. 9697 TSE Prime)

Notice and Apology Regarding Customer Information Affected Through Unauthorized Access

Capcom Co., Ltd. (Capcom) has determined that certain customer information associated with CAPCOM ID[*1], an online membership account service operated by the company, was subject to unauthorized access by a third party. Capcom sincerely apologizes for the complications and concern this has caused its customers and other stakeholders.

(*1 CAPCOM ID is a unified account that registrants can use to access various web services, and which is needed to play certain Capcom games online.)

Capcom has completed the necessary emergency response measures, and services that use CAPCOM ID remain available for use. Additionally, this incident does not affect players' ability to access or play any of our games. The facts confirmed at this time and the company's response to the incident are outlined below.

1. Overview of Information Affected (as of October 22)

(1) Email address records, system-specific identifier information[*2]

Number of affected records: 11,774,247 records (worldwide total)

(*2 Date and time of account creation, date and time of last login, number of logins, client IP address used during last login)

(2) Records of date of birth, gender, country/region, and nickname

Number of affected records: of the total in (1), 43 records

(3) Unauthorized changes to CAPCOM ID account login passwords

Number of affected accounts: of the total in (1), 196 accounts

Capcom has not confirmed any compromise of CAPCOM ID account login passwords originally set by customers themselves. However, the company has confirmed that passwords were changed without authorization on 196 accounts. The passwords associated with these accounts have already been reset, and the company continues to investigate the scope of any impact resulting from this incident.

Going forward, Capcom will notify customers affected by this incident. Credit card information was not included among the affected information.

2. Timeline of Events

October 19, 2026

Capcom detected suspicious activity indicating potential unauthorized access to CAPCOM ID and immediately began blocking the access while investigating the cause and scope of the incident. On the same day, the company confirmed that unauthorized access had occurred. In response, the company implemented emergency measures and proceeded with identifying and addressing the method of attack.

October 20, 2026

Capcom established an internal incident response headquarters and continued information gathering and measures to prevent further impact. As a result of the investigation, Capcom confirmed that certain customer information registered with CAPCOM ID had been subject to unauthorized access. The company also confirmed that passwords associated with a limited number of accounts had been changed without authorization. On the same day, Capcom reported the matter to the Information Technology Security Oversight Committee, the company's external advisory body.

October 21, 2026

Capcom reported the incident to the Osaka Prefectural Police and Japan's Personal Information Protection Commission. The company continues to monitor the situation, investigate the incident, and assess the full scope of the impact.

3. Advisory to Customers

Email addresses registered with CAPCOM ID may continue to be used without interruption. However, there is a possibility that the affected information could be misused to send fraudulent emails or other communications impersonating Capcom or related parties. If you receive any suspicious email or message, please exercise caution and refrain from accessing any URLs contained therein or opening any attached files.

4. Capcom's Response and Next Steps

Capcom has completed emergency response measures and has identified and addressed the attack method involved in this incident. Services that use CAPCOM ID, including games, remain available. Going forward, the company will begin contacting affected customers and has established dedicated customer-support channels for inquiries regarding this matter.

Data Security Incident Dedicated Customer-Support Channels

Japan

Dedicated Capcom ID Data Security Incident Support Line

Telephone (toll-free): 0120-801-271

Hours: 10:00 a.m. to 8:00 p.m. (JST)

North, Central and South America

Capcom USA Customer Support Page

Inquiry Form: https://www.capcom-support.com/hc/en-us/requests/new

Europe, Middle East and Africa (EMEA)

Capcom Europe Customer Support

Inquiry Form: https://www.capcom-support.com/hc/en-us/requests/new

Email: feedback@capcom.com

Asia (excluding Japan) and Oceania

Capcom Asia Customer Support

Email: info-asia@capcom.com

Capcom takes this matter extremely seriously and will continue its detailed investigation. Based on the findings of the investigation, it will implement measures to prevent recurrence and further strengthen its information security framework. Should any additional facts requiring disclosure be identified, Capcom will promptly provide updates through the company's official website and other appropriate channels.

Capcom would once again like to express its sincere apologies to its customers and all other stakeholders.

Inquiries regarding the above information may be directed to:

Media / Investor Contact

Capcom Co., Ltd.
Public Relations and Investor Relations Section
(Address) 3-1-3, Uchihiranomachi, Chuo-ku, Osaka, 540-0037, Japan
(Tel)+81-6-6920-3623 (Fax) +81-6-6920-5108