DATA BREACHES SECURITY

Burger King Japan Data Breach Impacts 11.18 Million App Member Records

BY DEEBA AHMED · OCTOBER 16, 2026 · 3 MINUTE READ

LISTEN TO THIS ARTICLE
Burger King Japan Data Breach Impacts 11.18 Million App Member Records
0:00
← 10s ▶ Play 10s →
Speed 1.25×
Voice Loading voices...
Press play to start listening

The Burger King Japan data breach occurred between October 2 and 7, exposing emails, birth dates and other data from nearly 12 million app members. Audit Security

BK Japan, the operator of **Burger King** restaurants in Japan, has confirmed a data breach in which personal information from about 11.18 million official app member records was stolen. The exposure occurred after a third party accessed BK Japan's membership system.

The company, operated by BK Japan Holdings Co., Ltd.and owned by Goldman Sachs Alternatives, disclosed the breach on October 15 in a press release, stating that the breach took place between October 2 and 7 while it discovered the leak on October 13.

Details of the Breach

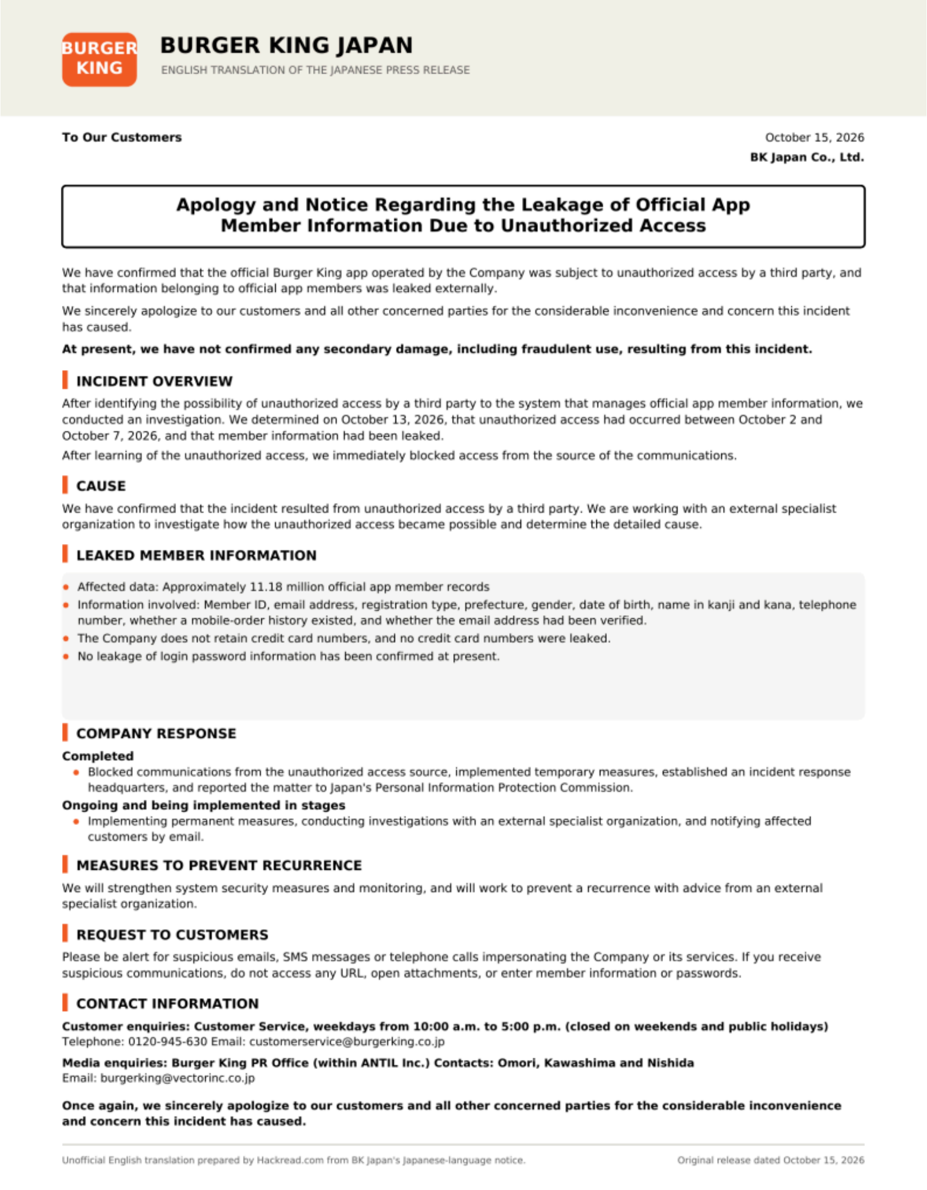
The exposed data includes customers' names in kanji and kana, phone numbers, email addresses, dates of birth, gender, prefecture and member IDs. Some records also contained registration details, email verification status, and information about mobile ordering.

BK Japan has not disclosed how the attacker gained access to the system. The reported mobile ordering data indicates whether a member had an order history, rather than revealing specific food orders.

Discover more
Audit Security
Data
Store Big Data

Company Response and Data Exposure

BK Japan's **press release** (PDF) stated that it does not store credit card numbers in the affected system, and no credit card numbers were exposed. The company also said it had not confirmed any leakage of login passwords. As of its announcement, no secondary harm, including fraudulent use of the leaked information, had been confirmed.



BURGER KING JAPAN
ENGLISH TRANSLATION OF THE JAPANESE PRESS RELEASE

To Our Customers

October 15, 2026
BK Japan Co., Ltd.

Apology and Notice Regarding the Leakage of Official App Member Information Due to Unauthorized Access

We have confirmed that the official Burger King app operated by the Company was subject to unauthorized access by a third party, and that information belonging to official app members was leaked externally.

We sincerely apologize to our customers and all other concerned parties for the considerable inconvenience and concern this incident has caused.

At present, we have not confirmed any secondary damage, including fraudulent use, resulting from this incident.

INCIDENT OVERVIEW

After identifying the possibility of unauthorized access by a third party to the system that manages official app member information, we conducted an investigation. We determined on October 13, 2026, that unauthorized access had occurred between October 2 and October 7, 2026, and that member information had been leaked.

After learning of the unauthorized access, we immediately blocked access from the source of the communications.

CAUSE

We have confirmed that the incident resulted from unauthorized access by a third party. We are working with an external specialist organization to investigate how the unauthorized access became possible and determine the detailed cause.

LEAKED MEMBER INFORMATION

- Affected data: Approximately 11.18 million official app member records
- Information involved: Member ID, email address, registration type, prefecture, gender, date of birth, name in kanji and kana, telephone number, whether a mobile-order history existed, and whether the email address had been verified.
- The Company does not retain credit card numbers, and no credit card numbers were leaked.
- No leakage of login password information has been confirmed at present.

COMPANY RESPONSE

Completed
- Blocked communications from the unauthorized access source, implemented temporary measures, established an incident response headquarters, and reported the matter to Japan's Personal Information Protection Commission.

Ongoing and being implemented in stages
- Implementing permanent measures, conducting investigations with an external specialist organization, and notifying affected customers by email.

MEASURES TO PREVENT RECURRENCE

We will strengthen system security measures and monitoring, and will work to prevent a recurrence with advice from an external specialist organization.

REQUEST TO CUSTOMERS

Please be alert for suspicious emails, SMS messages or telephone calls impersonating the Company or its services. If you receive suspicious communications, do not access any URL, open attachments, or enter member information or passwords.

CONTACT INFORMATION

Customer enquiries: Customer Service, weekdays from 10:00 a.m. to 5:00 p.m. (closed on weekends and public holidays)
Telephone: 0120-945-630 Email: customerservice@burgerking.co.jp

Media enquiries: Burger King PR Office (within ANTIL Inc.) Contacts: Omori, Kawashima and Nishida
Email: burgerking@vectorinc.co.jp

Once again, we sincerely apologize to our customers and all other concerned parties for the considerable inconvenience and concern this incident has caused.

Unofficial English translation prepared by Hackread.com from BK Japan's Japanese-language notice. Original release dated October 15, 2026

Burger King Japan published the original press release in Japanese. Hackread.com used AI to create this unofficial English translation for easier understanding. The translation may contain errors, so the original Japanese notice remains the authoritative version.

After identifying the unauthorized access, the company blocked connections from the source involved and established a response team. BK Japan reported the breach to Japan's Personal Information Protection Commission and is working with security experts to find out how the attacker got into the system. The company apologized to customers over the leak. Audit Security

With names, phone numbers, email addresses and dates of birth exposed, affected customers may face more convincing phishing attempts. Hackread.com reported a similar concern after **Revolut disclosed a data breach** and phishing messages targeting its customers emerged. However, researchers did not establish whether the messages were connected to the breach.

Expert's Comments:

Ensar Seker, CISO at cybersecurity company SOCRadar, shared his comments with Hackread.com, warning that the risks could extend beyond the initial breach.

"The risk extends beyond the initial breach. Names, dates of birth, email addresses and phone numbers can help criminals make fraudulent messages feel credible. An attacker could impersonate Burger King support, reference the breach and ask a customer to 'secure' their account through a fake verification page. That is a plausible follow-on threat, rather than evidence that such a campaign has already occurred," Seker said.

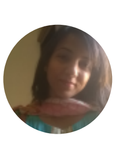
Discover more
data
Browse Reference
Earn a CS Degree

He also warned that seemingly minor account details could help scammers tailor their messages. "Knowing whether someone used mobile ordering could help tailor a convincing message without knowing what they actually purchased."

Seker advised customers to open the official app or website directly to check security notices and never share passwords or verification codes with someone who contacts them.

"For businesses, this reinforces why customer profile data deserves strong protection alongside credentials and payment information. Collecting less data, limiting access to member databases and detecting unusual bulk retrieval can reduce the impact of a compromise. Account recovery also needs protection: knowing a customer's birthday or phone number should never be enough to establish their identity," he added. Store Big Data

Deeba Ahmed



Deeba is a veteran cybersecurity reporter at Hackread.com with over a decade of experience covering cybercrime, vulnerabilities, and security events. Her expertise and in-depth analysis make her a key contributor to the platform's trusted coverage.

View Posts

Burger King · Cyber Attack · Cybersecurity · data breach · Japan · Privacy · security

View Comments (0)

Subscription Form

Email Address*

FIRSTNAME

LASTNAME

Subscribe

Latest Posts

US Ransomware Negotiator Suspected of Helping ShinyHunters Extort Victims

Bright Security Introduces STAR Fuzzer, Agentic Fuzzing That Writes Its Own Harnesses and Proves Every Finding

Fake Calendar Invites Target 40,000 Firms in Microsoft Credential Theft

OpenAI Model Hacked Crypto Wallet and Spent Funds to Deploy Smart Contracts

Claude Code Desktop Flaw Let Malicious HTML Steal Developer Credentials

PRESS RELEASE

PRESS RELEASE
Bright Security Introduces STAR Fuzzer, Agentic Fuzzing That Writes Its Own Harnesses and Proves Every Finding
BY CYBERNEWSWIRE

PRESS RELEASE, ARTIFICIAL INTELLIGENCE
FLock.io Unveils Edge Decision Model, Built on Qwen, for Enhanced Data Privacy
BY OWAIS SULTAN

PRESS RELEASE, ARTIFICIAL INTELLIGENCE
SerpApi Expands Beyond Search Results with New Extract API
BY OWAIS SULTAN

PRESS RELEASE
Criminal IP to Showcase Threat Intelligence and AITEM at Security Days Fall 2026 Tokyo
BY CYBERNEWSWIRE

PRESS RELEASE
G2A.COM Reports 35% Growth in Security Software Orders, Outpacing VPN Growth
BY CYBERNEWSWIRE

Related Posts

NEWS, CYBER ATTACKS, SECURITY
Israel Faces Fresh Wave of Cyberattacks Targeting Critical Infrastructure
Authorities believe that these cyberattacks may be part of OpIsrael, organized by pro-Palestinian hackers.
BY WAQAS

MALWARE, SECURITY
Evrial Info-Stealing Trojan Modifies Addresses to Steal Cryptocurrency
It is just another with just another Cryptocurrency malware targeting unsuspecting users – This time, it modifies addresses to...
BY WAQAS

SECURITY, SCAMS AND FRAUD
New AkiraBot Abuses OpenAI API to Spam Website Contact Forms
Cybersecurity researchers have identified a new spam campaign driven by 'AkiraBot,' an AI-powered bot that targets small business...
BY WAQAS

LEAKS, SECURITY
Unprotected MongoDB: Medical Data of Veterans affected by sleep disorders leaked
MongoDB database is being used by high-profile platforms worldwide but recently it is in the news for all...
BY WAQAS

READ

HackRead is a news platform covering Cybersecurity, AI, InfoSec, Cyber Crime, and Hacking News, along with in-depth reviews on Crypto and Technology trends. Founded in 2011, HackRead is based in the United Kingdom. Hackread.com, a GRAY DOT MEDIA GROUP LTD site. Copyright © 2026 HackRead

Privacy and cookie settings
Managed by Google. Complies with IAB TCF. CMP ID: 300

How your data is used
Your privacy preferences are important. That's why, based on legitimate interest, we and our partners process and share only limited data such as your device type and content interactions for advertising, research and service development purposes.
View partner list and manage privacy settings.