

October 23, 2026

Sompo Japan DC Securities Inc.

Notice Regarding a Possible Leak of Customer Information Due to Unauthorized Access to a Third-Party Email Delivery Service

Sompo Japan DC Securities Inc. (hereinafter referred to as “the Company”) uses “Blastmail,” an email delivery system provided by RAKUS LightCloud Co., Ltd. (hereinafter referred to as “the Service Provider”), to send notifications to participants and those who give investment instructions only (hereinafter referred to as “the Participants”) in defined contribution (DC) pension plans. The Company has learned that the servers of this system were accessed by an unauthorized third party, and that our customers’ information may have been leaked.

At this time, no unauthorized use of the information resulting from this incident has been confirmed. However, as the possibility of a leak cannot be completely ruled out, we are providing an overview of the incident and its current status.

The Company’s own systems were not accessed, and our DC pension services, including the “AnswerNet,” have not been affected.

The Company sincerely apologizes to its customers, plan sponsors, and all other stakeholders for the concern and inconvenience this has caused.

1. Overview of the Incident

In the early hours of October 21, 2026, the Service Provider notified the Company that it had detected suspected unauthorized access to its system and had suspended all of its services as an emergency measure.

A specialist team at the Service Provider is currently conducting a detailed investigation.

2. Information Potentially Affected

The potentially affected information is limited to data registered in the Service Provider’s system or stored in its delivery history.

(1) Affected Customers

Participants who have received notification emails from the Company since September 2022

(2) Types of Information

- Number of records: Up to approximately 250,000
- Items:

- Email addresses
- Names (approximately 10,000 of the above records only, where names were included in the delivery history)

(3) Information Not Affected

Addresses, phone numbers, dates of birth, Basic Pension Numbers, “AnswerNet” login IDs and passwords, financial institution account details, and asset balances were never stored on the affected servers and are therefore not at risk.

3. Next Steps

Once the Service Provider’s investigation has established the facts, the Company will individually contact any customers whose information is confirmed to have been leaked.

If you receive a suspicious email claiming to be from the Company, please do not click any links (URLs) or open any attachments. Delete the email immediately.

Contact

AnswerCenter

Via phone: 0120-401-593

From overseas: +81-3-5325-6303 (charges apply)

Business Hours: Weekdays: 2:00 PM to 6:00 PM

(excluding national holidays, year-end/New Year, and maintenance days)

Via online form

https://www.faq.sjdc.co.jp/helpdesk?category_id=3&faq_id=&site_domain=english

