April 27, 2026
ALPS ALPINE CO., LTD.

Notice Regarding Unauthorized Access to Personal Information

ALPS ALPINE CO., LTD. (the “Company”) has confirmed an incident in which an external VPN system used by the Company was subject to unauthorized access, and the possibility cannot be ruled out that personal information was viewed by an external attacker.

We sincerely apologize for the concern caused to all potentially affected individuals and other parties concerned.

The Company is continuing its investigation into this incident. The following information is being disclosed based on the facts currently known. Apart from the personal information that may have been subject to the unauthorized access described above, the Company has not confirmed any unauthorized access to customer information, business partner information, or other information of the Company or its group companies. At this time, the Company has not confirmed that such information was viewed by any external party or leaked outside the Company.

1. Overview of the Incident

On April 3, 2026, the Company received notice from a service provider entrusted with the maintenance and management of the Company’s internal systems that traces had been identified of unauthorized access by an external party to an external VPN system used by the Company.

On April 13, as a result of subsequent investigations conducted by the service provider, it was confirmed that unauthorized access had also been made to the Company’s server. The Company further confirmed that it cannot completely rule out the possibility that personal information of persons registered in the system for access to the Company’s internal systems was viewed from outside the Company.

The Company has not confirmed that customer information, business partner information, or other information other than the above was stored in the relevant system. At this time, the Company has not confirmed that such information was viewed by any external party or leaked outside the Company.

2. Information That May Have Been Affected

At this time, the information that may have been affected consists of the following personal information of officers, employees (including former employees), and others registered for access to the systems of the Company and its group companies, as well as certain employees of contractor companies:

- Login IDs (including some employee numbers)
- Names
- Company email addresses
- Job titles
- Department names
- System IDs

Passwords are managed in encrypted form, and at this time the Company has not confirmed that any such passwords were obtained through the unauthorized access. The Company has also confirmed that sensitive personal information, such as credit card information, bank account information, and Individual Numbers (“My Number”), was not stored in the relevant system.

3. Cause and Status of Investigation

The Company has confirmed that the cause of this incident was unauthorized access to an external VPN system used by the Company. The Company is continuing a detailed investigation into the cause in cooperation with external specialists.

4. Measures Taken to Date

After becoming aware of this incident, the Company promptly implemented the following measures:

- Suspension of use of the relevant system and review of its security settings
- Technical investigation by external specialists
- Explanation of the situation to relevant parties within the Company and its group companies
- Consultation with and reporting to relevant authorities, and consideration of necessary measures

5. Measures to Prevent Recurrence

The Company takes this incident seriously and, based on the results of the investigation, will sequentially implement the following measures to prevent recurrence:

- Strengthening of security measures and monitoring systems for the overall system environment, including VPN systems
- Re-examination of rules for the handling and management of personal information
- Ongoing information security education for users of internal systems

6. Future Response

If any new facts requiring disclosure are identified, the Company will promptly announce them.

At this time, the Company has not confirmed any secondary damage, such as unauthorized use of personal information resulting from this incident. However, we ask that you remain cautious regarding suspicious emails, contacts, or other communications impersonating persons related to the Company.

In light of the fact that the leaked information described above primarily relates to employees (including former employees) of the Company and its group companies, the Company has already notified employees of the Company and its group companies to change their passwords for internal systems as a precautionary measure.

7. Contact

For inquiries regarding this matter: Corporate Communications Department

Tel: +81-50-3613-1581 (Public Relations)

https://www.alpsalpine.com/e/common/inquiry.html