November 16, 2026

Company Name	PLAID, Inc.
Representative	Kenta Kurahashi, Representative Director and CEO (Code No.: 4165 TSE Growth)
Contact	Takahiro Tsuji, Executive Officer and CFO (TEL +81-3-4405-7597)

Notice and Apology Regarding the Leakage of Information Potentially Including Personal Information Due to Unauthorized Access

As announced on November 13, 2026, KARTE, a service provided by the Company, was subject to unauthorized access by a third party. Our investigation has confirmed that some of the information entrusted to us by companies using KARTE (hereinafter, "Client Companies"), which may include personal information, has been leaked.

We take very seriously the fact that this incident has occurred with information that was entrusted to us. We sincerely apologize for the significant inconvenience and concern this has caused our Client Companies, their customers and all other parties concerned.

We have contacted each affected Client Company individually. We are also reporting the matter to the Personal Information Protection Commission and consulting with the police.

1. Overview and Background of the Incident

In the early hours of November 13, 2026, a third party exploited a vulnerability in our servers to steal authentication credentials used to connect to our systems and databases, and exfiltrated data from those databases and other sources. Using the stolen credentials, the third party also took over a Company account and gained unauthorized access to the KARTE administration console.

We detected the unauthorized access at 8:59 a.m.(JST) the same day. To prevent further damage, we invalidated the stolen credentials, among other measures, and began shutting down our servers at around 2:27 p.m.(JST) We also switched all KARTE services to maintenance mode and shut them down one by one. Alongside this, we took containment measures, including invalidating the credentials used in the unauthorized access and blocking communications from the source of the attack. These measures were completed by around 3:23 p.m.(JST) the same day.

Since the source of the attack was blocked, we have found no further unauthorized access to our systems. All services remain suspended while we continue to investigate the scope of the impact.

2. Information Confirmed to Have Been Leaked

The information confirmed to have been leaked at this time is as follows.

(1) Email addresses registered to KARTE accounts: 79,249

(2) Credentials used to integrate KARTE with external services (secret keys, access tokens, etc.)

This affects Client Companies that have set up integrations with external services through the KARTE administration console or other means.Please note that the exact number of affected cases is currently under investigation.

(3) Part of the customer data (membership information, etc.) that Client Companies imported from their own records for use in KARTE (including data imported via KARTE's "Linked Table" feature)

Client Companies decide which fields to import, so this data may include personal information, depending on what

was imported.Please note that the exact number of affected cases is currently under investigation.

The fields that each Client Company links or sends to KARTE vary. We are continuing to investigate the full scope of the impact and any impact on other data entrusted to us through KARTE.

3. Request to Client Companies

If you use KARTE's integration features with external services, please revoke the relevant integration credentials to prevent further damage. If you have not yet done so since our individual notice, please do so as soon as possible. If these credentials are not revoked, unauthorized access to the connected services may result in unintended data being written to them, data leakage or other damage.

Emails impersonating the Company may also be sent to email addresses registered to KARTE accounts. Do not open links or attachments in unexpected emails, and do not enter your login information.

4. Outlook

We will continue to investigate the leaked information to determine the full scope of the impact, and will contact the affected Client Companies as new findings come to light. We also plan to commission an external security investigation to carry out a forensic analysis and to prepare for the resumption of services.

We have not yet decided when KARTE services will resume. We will announce this once a timeline has been established.

Based on the findings of the investigation, we will put in place measures to prevent a recurrence and announce them. If any new facts come to light in the meantime, we will announce them promptly.

5. Impact on Financial Results

We are currently assessing the impact of this incident on our financial results for the fiscal year ending December 31, 2026. We will promptly disclose any matters that require disclosure.

[Previous Announcement Regarding This Matter]
November 13, 2026 | Notice Regarding Unauthorized Access to Our Service
https://pdf.irpocket.com/C4165/xoA3/Laiu/qCUD/GL0K.pdf