

26 October 2026

KOMOJU Co., Ltd.
1-14-9 Kichijoji Honcho, Musashino-shi, Tokyo
9F, PLAFUS Kichijoji Front
CEO: Satoru Osawa

[Second Report] Personal Data Breach in Our CRM System

In our initial report dated 22 October 2026, we reported that an unauthorized third party had gained access to the CRM system used in our business operations (referred to as “Affected System 2” in the initial report), and that we were investigating the details of the scope of impact. Our investigation has now confirmed that some of the records we used in handling inquiries from merchants, business partners, and customers were leaked, and that these records contained personal information.

We sincerely apologize for the considerable concern and inconvenience this incident has caused to all those affected.

Details

Overview of the Incident

As stated in our initial report, an external third party gained unauthorized access to our non-production environment from the evening of 13 October 2026 onward. We confirmed that a security vulnerability in our non-production environment was exploited to log in without authorization to our internal administration interface and certain systems.

Our subsequent investigation confirmed that the third party also gained unauthorized access to our CRM system by using an API key used to connect our systems to the CRM system.

The CRM system stores records that we maintain in the course of handling inquiries from merchants, business partners, and customers, including consumers. This incident concerns a leak from the CRM system and is separate from the leak from Affected System 1 (the KOMOJU payment system) described in our initial report.

Information Leaked

Scope of Information Obtained by the Third Party

The third party used the above-mentioned API key to access the CRM system through its API and obtained information contained in inquiry records. We have not confirmed any extraction or export of bulk data—such as customer lists—nor of the CRM system's entire database.

Categories of Personal Data Subject to an Actual or Potential Breach

Inquiry history, email addresses, names, telephone numbers, addresses, dates of birth, bank account information, and official identification documents

The individuals concerned are officers and employees of our merchants and business partners, including payment partners, as well as consumers using our merchants' services, who have previously contacted us about payments processed through our services.

The categories of personal data concerned vary depending on the content of the inquiry. Bank account information is limited to information associated with payment refunds and similar matters. Official identification documents relate only to individuals who submitted them by email, primarily during the screening of merchants for use of our payment services. Other information is likewise limited to information provided in the course of an inquiry.

The above describes the categories of personal data involved in the CRM system leak. This is a separate incident from the approximately 4,100 cases involving Affected System 1 described in our initial report. We will contact the individuals affected by this breach individually.

Our policy is not to record credit card numbers in inquiry records and to delete them immediately if they are included in an inquiry or similar communication. Our investigation has confirmed that the information leaked in this incident did not include credit card information.

Status of Secondary Harm

At present, we have not confirmed any unauthorized payments or other secondary harm resulting from this incident. We have also not identified any evidence indicating that the leaked data has been used, or will be used, for unlawful purposes.

To Our Merchants

The information leaked in this incident is information that we use for purposes we have independently specified; it does not include information that merchants have entrusted to us for processing. Accordingly, we will handle the response to this breach, including notifying the individuals whose personal information was leaked and reporting to the Personal Information Protection Commission. No specific action is required of merchants in relation to this incident.

If you receive any inquiries from your customers or other related parties, please direct them to the dedicated contact point below.

Precautions

To minimize potential harm that may arise in the future, we recommend taking the following precautions.

- Exercise particular caution with unsolicited emails, text messages, and telephone calls from unknown parties or suspicious sources.
- If you are asked to provide sensitive information, such as passwords, financial information, or verification codes, do not respond immediately. First verify that the request is legitimate.
- Beware of suspicious emails or communications impersonating KOMOJU or our merchants. We will never ask for your password or authentication information by email, telephone, or similar means.

Next Steps

If further developments in our investigation or other circumstances give rise to additional matters that should be communicated, we will promptly publish them on the official KOMOJU website and notify affected individuals and merchants individually.

Contact Information

KOMOJU Co., Ltd. — Dedicated Contact Point for This Incident

Email : security-contact@komoju.com