

Note: This document has been translated from the Japanese original for reference purposes only.
In the event of any discrepancy between this translated document and the Japanese original,
the original shall prevail.



October 15, 2026

To whom it may concern:

Company: ACCESS CO., LTD.
Representative: Tsutomu Yoshioka
Representative Director, President & CEO
(Securities Code: 4813 Prime Market, TSE)
Contact: Ryuji Natsuumi
Senior Executive Officer and Director, CFO
(Phone: +81-3-6853-9088)

Notice Regarding Unauthorized Access and Personal Information Leakage **at a Consolidated Subsidiary**

ACCESS CO., LTD. hereby announces that the Company confirmed that unauthorized access by a third party occurred within "CROS", a business support service provided by its subsidiary, ACCESS AP TAIWAN Co., Ltd. (hereinafter "AP Taiwan"), for e-commerce businesses expanding internationally. This incident resulted in the leakage of personal information belonging to customers who used e-commerce services operated by AP Taiwan's client companies. Furthermore, it has been determined that information stolen from the compromised server was used to send unauthorized emails to third parties.

The Company sincerely apologize for the significant inconvenience and concern this has caused to our customers, business partners, and all other affected parties.

1. Background

On September 11, 2026, AP Taiwan detected signs of unauthorized access to a server used for "CROS." In response, they immediately shut down and isolated the affected server and initiated an investigation. AP Taiwan has since determined that a third party gained unauthorized access and carried out an attack, resulting in the illicit acquisition of certain personal and configuration data that could be accessed via that server. The Company issuing this notification to inform you of the incident.

Furthermore, our investigation revealed that unauthorized access originated from a Business Intelligence (BI) tool that had been provided exclusively to one of our client companies using "CROS." As of now, no data breaches involving personal information related to any other client companies have been identified.

2. Leaked Personal Information, etc.

The main information confirmed to have been leaked as of this time is as follows:

(1) ID-related

Customer IDs: 155,280

Order IDs: 231,998

Data fields: Name, phone number, address, email address, and associated order information

Target regions: Taiwan, Hong Kong, Macau, Singapore

(2) Credit card-related

Total count: 1,671

Unique accounts: 1,305 (after consolidating duplicate registrations and multiple orders)

Data fields: Credit card number, security code, expiration date, name, associated customer ID,

and associated order ID

Notes:

1. In 4 of these cases, all data fields were compromised; for the remaining 1,301 cases, all information except the security code was compromised.
2. The compromised credit card information pertains only to orders for which credit card payment had not been completed.

(3) Payment service-related

Data fields: Account information for the payment services used

(4) Others

Unauthorized email distribution: 11,441 instances

Note:

Based on an analysis of the email data, it has been determined that the compromised personal information itself was not used for these unauthorized emails. Instead, the unauthorized party used a separate list they had prepared, along with email service access keys stolen from the compromised server, to send the emails.

3. Response Status and Measures to Prevent Recurrence

Following the discovery of this incident, AP Taiwan has implemented the following measures:

- Isolation and emergency shutdown of the servers affected by the unauthorized access.
- Invalidation and updating of credentials used for email transmission.
- Temporary suspension of the entire CROS service—including services for other business partners—to prevent secondary damage, along with a change of database passwords (services have since been restored).
- Implementation of masking for credit card information across all clients within the active systems.
- Updating of secret keys for payment services (partially completed; remaining work is in progress).

In addition to the above, the following measures are planned to prevent a recurrence:

- Modifying the CROS program to ensure that credit card information is not retained for transactions that have not yet been completed (note: such information is already not retained for completed transactions).
- Support from security and server specialists at the Company to assist in the implementation and verification of enhanced security measures.

Following an investigation and log analysis conducted after the discovery of this incident, the Company has determined that unauthorized access occurred at the application level of the aforementioned BI tool. Furthermore, no impact has been detected on databases outside of those accessible via this tool, nor has there been any direct intrusion into the underlying infrastructure of the "CROS" system itself.

The service providers (business partners of AP Taiwan) that utilize the affected BI tool are taking necessary measures, including reporting the incident to the Personal Information Protection Commission. In addition, AP Taiwan has submitted a report to the relevant authorities in Taiwan. Service providers are also notifying the customers who use their e-commerce services. Throughout these processes, AP Taiwan has been providing the necessary information and technical support to its business partners.

4. Future Outlook

The Company anticipates that the impact of this matter on its consolidated financial results will be minor; however, currently conducting a detailed assessment. Should any developments arise that require disclosure, the Company will announce them promptly.