

Translation: Please note that the following purports to be an accurate and complete translation of the original Japanese version prepared for the convenience of investors. However, in the case of any discrepancy between the translation and the Japanese original, the latter shall prevail.



October 23, 2026

For Immediate Release

Corporate Name PARK24 CO., LTD.
Securities Code 4666, Prime Market of TSE (Ticker Symbol: PKCOY)
Representative Koichi Nishikawa
President and Representative Director, CEO
Contact Takao Miki
Director Executive Corporate Officer, CFO
(TEL: +81-3-6747-8120)

Notice Regarding Investigation Results Concerning Unauthorized Access and Future Measures

On September 28, 2026, PARK24 CO., LTD. announced in the “Notice Regarding Unauthorized Access at a Consolidated Subsidiary's System and Personal Data Breach” the detection of unauthorized access by a third party to the web system of the Times CAR car-sharing service operated by our consolidated subsidiary, TIMES MOBILITY CO., LTD. (“Times Mobility”), resulting in the breach of certain personal information held by the Group (the “Incident”).

We have been conducting a forensic investigation of the Incident through an external specialist and have received a completed report of the investigation. We hereby announce the facts identified through the investigation, the scope of impact, and the cause of the Incident, as well as the future measures determined today, as set forth below.

We sincerely apologize for the significant inconvenience and concern caused to our customers, business partners, and all other stakeholders.

1. Developments Since the Incident

On September 25, 2026, the Group detected abnormal access to the Times CAR web system and immediately began an investigation and containment measures.

After confirming the possibility of unauthorized access, we isolated the affected systems, blocked the access route, analyzed logs, and conducted a forensic investigation through an external specialist. We have reported the Incident to the Personal Information Protection Commission, and successively notified affected customers, and made public announcements.

We also established a dedicated inquiry desk for customer, and are considering measures to prevent future harm, response policy, while continuing to monitor for actual damage related to the Incident.

The principal developments are as follows:

Date	Response
2026/9/25 (Fri.)	Detected unauthorized access by a third party and immediately began an investigation
	Isolated the affected server
	Blocked the unauthorized access route
	Began a forensic investigation through an external specialist
	Established an inquiry desk
	Reported to the Personal Information Protection Commission
2026/9/26 (Sat.)	Published the first report on the website, stating the possibility of breached personal information
	Completed separation of the compromised environment and related environments
2026/9/28 (Mon.)	Updated the first report
	Began notifying existing members
2026/9/28 (Mon.)	Published the “Notice Regarding Unauthorized Access at a Consolidated Subsidiary's System and Personal Data Breach”

	Published the second report on the website
	Began consulting with the police
	Reported to the Ministry of Land, Infrastructure, Transport and Tourism
2026/9/29 (Tue.)	Published the third report on the website
	Began notifying individual members
2026/10/1 (Thu.)	Began notifying former members
2026/10/2 (Fri.)	Began notifying corporate members
2026/10/16 (Fri.)	Published the fourth report on the website
2026/10/23 (Fri.)	Completion of forensic investigation by external specialist
	Published investigation results and response policy

2. Investigation Results

The forensic investigation conducted by the external specialist identified the following facts.

(1) Cause of the Incident

We have determined that the Incident was caused by an exploit on the vulnerability in the web system. The attacker exploited this vulnerability and searched for information within the system and used the information obtained to access our database and file storage areas.

To prevent secondary damage, we will refrain from disclosing details of the attack method and system configuration.

(2) Information confirmed to have been breached or potentially breached, and scope of impact

Unauthorized access to the Times Club web system was also confirmed in connection with the Incident. We previously announced that approximately 1.60 million identity verification document images may have been breached. Detailed investigation confirmed the trace of access and external transmission of approximately 1.46 million identity verification document image data. The investigation also identified traces of access on encrypted data by the attacker, although no traces of external transmission were found.

The number of affected accounts and information currently confirmed are as follows.

[Breached Accounts from the Times CAR web system]

①	Confirmed data for which the information on the right column showed traces of access and external transmission by the attacker	<ul style="list-style-type: none"> • Name*1 • Address • Date of birth • Telephone number*1 • Email address*1 • Driver's license information 	6,628,007 Accounts
---	--	---	--------------------

*1 Contract information for Times Business Service customers who enrolled through "Kantan Nyukai" (simplified enrollment) is managed in the Times CAR web system. As a result, the affected data includes information on Times Business Service customers who have contracts solely for parking services.

<Breached Identification and Attribute Information Among the Accounts Included in ①>

②	Identification and Attribute Information data for which traces of access and external transmission by the attacker were confirmed	Department name of corporate member	3,677 Accounts
		Times CAR membership number (IC Management number)	8 Accounts
		Times Business Card number	113 Accounts
		Linked-service ID*2	4 Accounts

*2 In the "Notice Regarding Unauthorized Access at a Consolidated Subsidiary's System and Personal Data Breach" published on September 28, 2026, we stated that 9 linked-service IDs including JR West Group membership service "WESTER ID" had been breached. The investigation determined that the actual number was 4. Furthermore, none of the WESTER IDs for West Japan Railway Company's membership service was found affected by the Incident.

<Breached Authentication Information Among the Accounts Included in ①>

③	Hashed Authentication Information data for which traces of access and external transmission by the attacker were confirmed	Passwords	4 Accounts
---	--	-----------	------------

<Breached Identity Verification Document Images Among the Accounts Included in ①>

④	Encrypted Identity Verification Document Image data for which traces of access and external transmission by the attacker were confirmed*3	1,464,800 Accounts
⑤	Encrypted Identity Verification Document Image data for which traces of access by the attacker were confirmed, but no traces of external transmission were found	891,602 Accounts
	Total	2,356,402 Accounts

*3 Because identity verification document image data were stored in encrypted form, confirmation of traces of access or external transmission by the attacker does not in itself mean that the image contents became immediately viewable. However, the possibility that externally transmitted encrypted data maybe decrypted in the future cannot be completely ruled out.

[Breached Accounts from the Times Club web system]

⑥	Confirmed data for which Information on the right column showed traces of access and external transmission by the attacker	<ul style="list-style-type: none"> • Name • Address • Date of birth • Driver's license information 	5 Accounts
		Times Club Card number	19,510 Accounts
		Times Business Card number	12 Accounts
		Linked-service ID*4	135,436 Accounts
		Last four digits of credit card number*5	28 Accounts

*4 This is an identification number used to link with third-party partner services offered through Time Club.

*5 The Group does not retain payment information and therefore does not retain full credit card numbers or security codes. Accordingly, there is no risk of unauthorized use.

Traces were also found indicating that the attacker accessed and externally transmitted identification information used for membership management and system operation.

The final numbers based on the investigation by the external specialist are as stated above, and no additional scope of impact has been identified at this time.

(3) Impact on Customers and Anticipated Risks

We are continuing to work with the external specialist to investigate the content of the breached information, developments around the externally transmitted information as well as any occurrence of secondary damage.

At this time, we have not identified any facts indicating that the information breached in the Incident has been sold or made public. However, because the breached information includes identity verification information in addition to personal information such as names and addresses, the following risks are anticipated.

- Fraud involving phishing emails or phishing websites
- Applications and inquiries made through impersonation
- Fraudulent solicitation
- Misuse of personal information

We will continue to work with the external specialist to monitor circulating information, including on the dark web, and verify whether any actual damage has occurred.

The Group does not retain payment information and therefore does not retain full credit card numbers or security codes. Accordingly, there is no risk of unauthorized use.

3. Future Response Measures

(1) Measures for Customers

We are implementing the following measures, giving the highest priority to preventing harm and alleviating customer concerns.

A) Notifying affected customers

We are individually notifying affected customers.

B) Establishing dedicated inquiry desk

We have established a dedicated inquiry desk for the Incident to receive inquiries and consultations from customers.

C) Consolation Payment (*Omimai-Kin*)

We recognize the significant concern and burden caused to customers for whom traces of access to and external transmission of encrypted identity verification document image data, including driver's licenses, were confirmed. Therefore, we have decided to provide consolation payments (*Omimai-Kin*) of 3,000 yen in the form of cash or cash equivalent vouchers.

Because these image data were stored in encrypted form, confirmation of traces of external transmission does not in itself mean that the image contents became immediately viewable. However, considering that the possibility of future decryption of externally transmitted encrypted data cannot be completely ruled out, as well as the impact and burden on customers, the consolation will be provided to those whose encrypted identity verification document image data, including driver's licenses, showed traces of access and external transmission.

The details and method of delivery of the consolation payment (*Omimai-Kin*) are currently under consideration and will be communicated to eligible customers once determined.

D) Ongoing response

If new facts are identified, we will provide additional information to affected customers and consider necessary response measures.

(2) Retention of Identity Verification Document Images

A) Rules revision for identity verification document image retention for Times CAR

The Group had retained encrypted image data of driver's licenses and other identity verification documents submitted by customers when registering for Times CAR membership throughout the membership period and 7 years after membership cancellation. These were retained for identity verification at registration, responding to suspected unauthorized use, handling inquiries, and other identity verification procedures.

Identity verification document images were stored and managed in accordance with internal rules. The retention period was also administered in accordance with the standards established by the Group.

In response to the Incident, after comprehensively considering the risks associated with retaining identity verification document images and the appropriate approach to their management, we revised our operations and internal rules so that images are no longer retained after completing membership registration.

	Before	After change
Current members	Retained during the membership period	Deleted immediately after completing registration verification
Former members	Retained for 7 years after membership cancellation	—

B) Deletion of identity verification document images

Previously, identity verification document images that were no longer required under internal rules were deleted, and images were also deleted upon request from the person concerned.

In conjunction with this revision of internal rules, all identity verification document image data currently retained by the Group will be deleted by the end of October 2026, regardless of whether the person concerned makes a request.

Although the image data will be deleted, information required to verify the identity of the images held by the Group has been appropriately preserved for future customer inquiries.

(3) Current response status

With respect to the Incident, we investigated the infiltration route, attacker's activity, impact, and have completed necessary measures to address the infiltration route.

We also inspected and implemented vulnerability countermeasures to systems with the same configuration, as well as introducing additional measures to strengthen monitoring and detection.

Necessary measures addressing the confirmed infiltration route have been completed at this time. We will continue to enhance our security measures and monitoring framework.

(4) Current response status and future response

We regard the Incident as a serious management issue and will advance initiatives to prevent recurrence and restore trust.

Considering advice from external information security experts, we will formulate and sequentially implement measures to strengthen information security.

In addition, we will establish an investigation committee centered around the Company's outside directors and external experts. This committee will examine the Incident from the perspective of the group's internal controls and governance.

We aim to announce specific information regarding security and governance enhancement measures by the end of the year.

4. Impact on Financial Results

Considering various costs and factors relating to the Incident, we have decided to revise the full-year consolidated financial results forecast for the fiscal year ending October 31, 2026. For details, please refer to the "Notice Regarding the Recording of Extraordinary Loss and Revision to the Full-year Consolidated Financial Results Forecast" released today.

5. Dedicated Hotline for Customers Affected by this Incident

- Toll-free Hotline: 0120-25-8924 (24 hours)

*Please ensure that you dial the correct number.

- Inquiry form (Only in Japanese): <https://share.timescar.jp/inquiry.html>