

[Translation]

October 6, 2026

Company Name: Mr Max Holdings Ltd.
Representative: Yoshiaki Hirano, President
(Code No. : 8203, TSE Prime)
Contact: Nobutaka Ueda, Executive Officer, Head of
Corporate Planning and Finance Division, and
General Manager of Finance Department
(Tel: +81-92-623-1111)

Notice and Apology Regarding Information Leakage Due to Unauthorized Access

We regret to announce that the servers for the MrMax App and online store (collectively, the "Services") operated by MrMax Corporation ("MrMax"), a subsidiary of the Company were subject to unauthorized access by a third party, and we have confirmed that part of the information held by MrMax has been leaked externally. We hereby report the facts identified to date and the measures taken by MrMax, as outlined below.

We deeply apologize to our customers and all other stakeholders for the considerable trouble and concern this incident has caused.

1. Timeline of Events

On the evening of Saturday, October 3, 2026, MrMax detected suspicious access to its servers. Immediately upon discovery, MrMax temporarily suspended the Services and, on the same day, took measures to block access from external sources. A subsequent investigation revealed that a third party had gained unauthorized entry to the servers by misusing a function of the software that makes up the Services, and that part of the personal information of registered members of the Services had been leaked.

2. Customers and Information Potentially Affected

Affected customers	Members of the MrMax App and members of the online store
Number of affected customers	Up to 1,735,154 (customers registered as members as of October 3, 2026)

Affected information Member ID, name, email address, and telephone number (*)

* The information affected varies depending on each customer's registration details.

MrMax has confirmed that addresses, dates of birth, credit card information, passwords, and purchase histories have not been leaked.

3. Request to Our Customers

As of the publication of this notice, no damage resulting from the misuse of the leaked information has been confirmed. However, spoofing or phishing emails may be sent using this information in the future. We kindly ask that you exercise caution, for example, by deleting suspicious emails without opening them or any attachments.

Please also be wary of any suspicious emails, text messages (SMS), phone calls, or postal mail claiming to be from MrMax or from persons associated with MrMax. MrMax will never ask you for your password or credit card number.

MrMax will notify each affected customer individually by email, together with its apology. Emails from MrMax will be sent from the following address: noreply@mrmax.jp

4. Response and Measures to Prevent Recurrence

MrMax has reported this incident to the Personal Information Protection Commission and has also consulted with the police.

In addition, MrMax has implemented measures to block the unauthorized access route. MrMax is currently conducting a detailed investigation with the cooperation of external specialists and has strengthened its monitoring system. Going forward, MrMax will reinforce the security of its systems based on the findings of the investigation and make every effort to prevent a recurrence. Should the investigation reveal any further facts requiring disclosure, we will announce them promptly.

5. Impact on Financial Results

The impact of this incident on our financial results is currently under review. Should it become apparent that this incident will have a material impact on our financial results, we will promptly disclose it.

【Inquiries Regarding This Matter】

Contact : incident-desk@mrmax.co.jp



We once again deeply apologize to our customers and all other stakeholders for the trouble and concern this incident has caused.

We take this matter extremely seriously and are and the entire Group is committed to preventing a recurrence and restoring trust.