August 31, 2026

Company name	COTA CO., LTD.
Representative	Shigeharu Yoshida Representative Director and President
Listing	TSE Prime Market
Securities code	4923
Point of contact	Mitsuhiro Nishimura Director, General Manager of Public Relations & Investor Relations Department (TEL +81-774-44-4923)

Notice Regarding Material Weakness in Internal Control over Financial Reporting to Be Disclosed

COTA CO., LTD. hereby announces that, in its internal control report for the 47th fiscal year (fiscal year ended March 31, 2026), submitted to the Kinki Local Finance Bureau on August 31, 2026, pursuant to Article 24-4-4, Paragraph 1 of the Financial Instruments and Exchange Act, the Company determined that a material weakness in internal control over financial reporting requiring disclosure existed and that its internal control was therefore not effective, as described below.

1. Details of the Material Weakness to Be Disclosed

On March 27, 2026, the Company experienced a system disruption after certain servers and other systems were infected with ransomware following unauthorized access (a cyberattack) by a third party. To prevent further spread of damage, the Company promptly implemented measures, including disconnecting all servers and other systems from the network.

In light of the seriousness of this situation, the Company established the Management Crisis Response Headquarters and, in collaboration with external experts, conducted a forensic investigation into the scope of the impact of the system disruption, the possibility of information leakage, and other relevant matters.

At the same time, the Company made the continuation of its financial closing operations its highest priority and sought the early restoration of its network and systems. However, due to the system disruption, the Company was unable to obtain the data and other information necessary to prepare its financial statements and therefore had to perform its financial closing operations manually and through other alternative methods. In addition, the audit procedures conducted by the auditing firm required more days than usual. As a result, the year-end financial closing process was delayed, making it impossible for the Company to file its Annual Securities Report within the statutory deadline.

As a result of reviewing the cause of this incident and countermeasures in light of the report from external

experts, the Company concluded that, although it had previously recognized the importance of cybersecurity and had implemented certain measures, its risk assessment and corresponding countermeasures were insufficient. In light of the seriousness of the situation that resulted in the delay in filing the Annual Securities Report, the Company determined that a material weakness requiring disclosure existed in its company-level internal controls and general IT controls.

2. Reason the Material Weakness Could Not Be Remedied by the End of the Fiscal Year

As the above facts were identified on March 27, 2026, when the cyberattack occurred, the Company was unable to remedy the situation by the end of the fiscal year.

3. Remediation Policy for the Material Weakness to Be Disclosed

The Company recognizes the importance of internal control over financial reporting and, in order to remediate the material weakness requiring disclosure, is further strengthening its cybersecurity by implementing the following measures to prevent recurrence.

(a) In collaboration with external experts, the Company has conducted a detailed forensic investigation and analysis to determine the attack vector, the scope of the impact, and the cause of the incident, and is promptly taking corrective measures to address the identified vulnerabilities.

(b) The Company has conducted comprehensive, system-wide inspections assuming a variety of attack methods and is striving to mitigate the risk of recurrence by identifying potential risks and prioritizing countermeasures.

(c) The Company has further strengthened its network and system monitoring framework and, through the introduction of security solutions and other measures, has established a framework that enables early detection of suspicious activity and prompt incident response.

The Company will strive to further strengthen its cybersecurity by steadily implementing these multi-layered measures while continuously reviewing and refining them in light of changes in the environment and emerging threat trends.

4. Impact on the Financial Statements

There is no impact on the financial statements for the fiscal year under review.

5. Audit Opinion in the Independent Auditor's Report on the Financial Statements

The auditing firm expressed an unmodified opinion.