July 22, 2026

Dear Valued Customers and Business Partners,

Subject: Investigation Results Regarding the Cyberattack Against Our Company

Thank you for your continued business and support.

In our announcement dated May 26, 2026, entitled “Report on Cyberattack Against Our Company,” and in our announcement dated June 12, 2026, entitled “Report on Cyberattack Against Our Company (Update),” we disclosed that our servers had been targeted in a cyberattack by a third party.

As previously disclosed, our information systems were subjected to a cyberattack (ransomware) by an external actor, which resulted in the encryption of certain internal servers. With the support of external experts, we have been investigating the scope of the impact, the cause of the incident, and the point of entry. We are writing to inform you that this investigation has now been completed, and we hereby report the findings below.

1. Investigation Results

(1) Timeline and Related Facts

- At around midnight on Sunday, May 17, 2026 (Japan Standard Time), we received an internal report indicating a system disruption affecting our servers. Following internal verification, we confirmed at around 9:30 a.m. on Monday, May 18, that data on the servers had been encrypted by ransomware.
- At around 10:00 a.m. the same day, in order to prevent any further spread of the damage, we disconnected our systems from the Internet and took isolation measures. We believe that the attacker’s activities ceased thereafter.
- We promptly worked with external experts to deploy investigative and monitoring tools across our systems, and conducted an investigation into traces of compromise while monitoring for any ongoing attack activity.

(2) Initial Intrusion

- As a result of the investigation, we found that it is highly likely that the attacker infiltrated our internal network via SSL-VPN and executed the ransomware.

(3) Indicators Suggesting Possible Data Exfiltration

- During the investigation, we identified traces remaining on our servers that indicate a high likelihood that files containing personal information and other data had been exfiltrated by the attacker.

(4) Categories of Data Highly Likely to Have Been Leaked

- Contact details of officers and employees of our customers, suppliers, and other business partners (names, telephone numbers, and email addresses)
- Technical and product information of our customers, suppliers, and other business partners, transaction-related information, pricing information, and information contained in business communications
- Personal information of our employees (including retirees), such as names, dates of birth, gender, addresses, telephone numbers, job titles, and family-related information (names, dates of birth, and gender)

At this time, we have not received any reports confirming any unauthorized use of the above information.

2. Important: Beware of Fraudulent Communications Impersonating Our Company or Its Officers and Employees

Please be aware that you may receive suspicious emails or telephone calls purporting to be from our company or its officers and employees. Under no circumstances should you respond to or comply with any requests or instructions contained in or made through such communications. Even if a communication appears to have been sent in our name or in the name of any of our officers or employees, please verify its authenticity by contacting us using the contact information set out below.

3. Measures to Prevent Recurrence and Reports to External Authorities

(1) Key Measures to Prevent Recurrence

- Based on the recommendations of external experts, we have rebuilt the relevant systems and reset or deleted compromised accounts, and have already implemented measures to eradicate the threats identified in our environment.
- We have also implemented various security enhancement measures, including continued monitoring through EDR introduced as part of our response to this incident and strengthened password management.
- The VPN believed to have been used as the point of entry has remained suspended since the incident. If and when it is resumed, we plan to introduce multi-factor authentication and change the VPN method to IPsec-VPN. We will continue to make improvements and implement additional measures to prevent recurrence and maintain secure operations.

(2) Reports to External Authorities

- On Thursday, July 16, 2026, we submitted a final report to the Personal Information Protection Commission regarding the matters confirmed through the investigation.
- We also continue to report to the police.

4. Contact Information

inquiries@koaglass.co.jp

Once again, we sincerely apologize for the significant concern and inconvenience this cyberattack against our company has caused our business partners and other stakeholders.

If any new material facts that should be communicated come to light, we will promptly notify you. We will continue to devote our full efforts to preventing any recurrence, and we sincerely appreciate your continued understanding and cooperation.

Koa Glass Co., Ltd.