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.

June 16, 2025

Dear customers,

Asuka Corporate Advisory Co., Ltd.

Aizawa Asset Management Co., Ltd.

Notice Regarding Leakage of Personal Information (Final Report)

Asuka Corporate Advisory Co., Ltd. (hereinafter referred to as, the "Company" or "ACA") discovered that there was a leak of personal information due to unauthorized access by a third party. The matter was announced on the websites of both ACA and Aizawa Asset Management Co., Ltd. (hereinafter referred to as Aizawa AM) on April 30, 2025.

In addition, a forensic investigation to identify the cause of unauthorized access by a third-party investigative agency (external security expert) was completed in a report dated May 28, 2025. On May 30, 2025, based on forensic and internal investigations, ACA and Aizawa AM completed the identification of the items of personal information that had been leaked. ACA hereby notifies you as follows.

ACA and Aizawa AM sincerely apologize to our customers for the significant concern and inconvenience this incident has caused. We take this matter very seriously and will do our utmost to implement measures to prevent a recurrence.

1. Overview of the leakage of personal information

On April 4, 2025, 108 spam emails were sent from the email address of an ACA director (hereinafter referred to as the "ACA officer"), and executives and employees of ACA and Aizawa AM as well as our business partners received the emails. ACA and Aizawa AM received an inquiry after receiving the email and began internal investigations at both companies.

Aizawa AM has been contracted to carry out a part of its business operations from ACA, and the ACA officer is also an executive officer of Aizawa AM.

After confirming this incident, ACA changed the password of the ACA officer on the same day as a measure to prevent the damage from spreading.

This incident may have resulted in leaking personal information~~,~~ because 444 of the emails stored on the ACA officer's email server were being downloaded or accessed.

2. The number of people whose personal information was leaked and the items of personal information that were leaked

The investigation discovered that personal information of 72 people had been leaked. The items of the personal information that were leaked are as follows.

・**Clients, etc. as financial instruments business operators**

ACA has no individual customers, as all are corporate clients. Personal information of employees of two of its corporate clients was leaked.

(1) Corporate clients: 10 people

◆Leaked personal information items

Name, address, telephone number, email address, information about workplace or affiliated organization and bank account, etc.

・**Those other than clients as financial instruments business operators**

Personal information of ACA executives and employees, their families, ACA-affiliated companies, old and new shareholders and employees of business partners was leaked.

(2) ACA (including executives and employees, families of executives and employees, retired people and auditors, etc.): 12 people

◆Leaked personal information items

Name, address, email address, information about workplace or affiliated organization, bank account, gender, face photo, family composition and relationship, etc.

(3) ACA-affiliated companies, old and new shareholders, business partners, etc.: 50 people

◆Leaked personal information items

Name, address, telephone number, email address, information about workplace or affiliated organization, bank account, gender, face photo, family composition and relationship, etc.

3. Cause of occurrence

The ACA officer implemented regular password changes and two-factor authentication. However, when a suspicious email was received in the email account of the ACA officer on March 27, 2025, the officer was urged to confirm a password. According to the ACA officer, the officer initially ignored the suspicious email, but the forensic investigation report indicated that it was highly likely that the officer clicked the URL in the suspicious email for some reason and accessed a phishing site inadvertently.

4. Presence or absence of secondary damage or its risk and its details

As a result of the internal investigations, ACA confirmed that the file attached to the spam email contained a virus when it was opened. For that reason, there is secondary damage or the risk of such damage as the following.

(1) There is a possibility that you may continue to receive spam emails using leaked email addresses and personal information.

(2) According to the internal investigation, when you receive a spam email and follow the instructions in the email, there is a risk of being infected with a virus (it is the result of a virus test performed on a PC with which Aizawa AM opened the email).

At the time ACA offered apologies and explanations to those to whom spam emails were sent, there had been no secondary damage. However, we would like to ask you to be careful if you receive any suspicious emails, since there is a possibility that spam emails may be sent by third parties using the leaked email addresses and personal

information in the future.

5. Status of implementation of response to those whose personal information was leaked

After the incident occurred, ACA promptly sent emails on April 7 to offer apologies and explanations to all those who received spam emails.

6. Status of publication

The first report was published on April 30, 2025, and this is the final report.

7. Measures to prevent recurrence

As measures to prevent recurrence, ACA will take the following measures for all executives and employees (some of which have been already implemented).

① Passwords of all ACA executives and employees have been changed (completed)

② In order to improve literacy on personal information and cyber security, we will offer training on internal response and communication system when receiving spam emails.

③ Based on the findings of the forensic investigation report, we have asked Aizawa AM to improve its operations before accepting operations from us in the future, and we have subsequently received an improvement report.

8. Other matters for reference

There was no leakage of “My Number” personal identification numbers. We also completed our reporting to the Personal Information Protection Commission on May 30, 2025.

<Contact information regarding this matter>

・Asuka Corporate Advisory Co., Ltd.

TEL: +81-3-6228-5097

・Aizawa Asset Management Co., Ltd.

Client Solution Division

TEL: +81-3-6263-9690

EMAIL: clientsolutions@aizawa-am.co.jp