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.

December 6, 2024
Aizawa Asset Management Co., Ltd.

Regarding the leak of personal information (final report)

Aizawa Asset Management Co., Ltd. (hereinafter referred to as the "Company") posted an announcement on its official website on May 31, 2024, in regard to a data leak following an unauthorized access by an outside party to an account held by the Company at a cloud email service provider.

On July 8, 2024, the forensics investigation to identify the cause of unauthorized access and follow-up investigation to specify downloaded emails were completed by a third-party investigation agency (an external security specialist).

Based on those investigations, we hereby notify you as follows that we have completed an internal investigation to identify the details of personal information leaked by the Company on Nov. 15, 2024.

We deeply apologize for any inconvenience or concerns caused to our customers. We have taken the situation seriously and will do our utmost to implement measures to prevent the recurrence of similar incidents. We also sincerely apologize that it has taken a long time to provide a final report, since the investigations involved a wide range of targets.

Details:

1. Background

On May 13, 2024, 811 spam emails soliciting investments were sent to our customers and related parties from a specific employee (hereinafter referred to as the "Affected Employee"), and we confirmed the occurrence of the situation after receiving the spam email. As we confirmed the situation, we changed the Affected Employee's password on the same day as measures to prevent further harm to our customers.

On May 15, 2024, we identified the situation where approximately two years' worth of the Affected Employee's emails stored on the Company's cloud email service provider were downloaded and leaked through multiple unauthorized access between April 28, 2024 and May 13, 2024. We sent emails to apologize to our customers and related parties who received spam emails on the same day.

2. The number and details of personal information that were leaked or may have been leaked

The investigation identified the personal information of 2,540 individuals was leaked. The details and number of personal information are as follows.

(1) Customers, etc. of the Company as a financial instruments business operator

Our customers with whom we have contracts as a financial instruments business operator.

◆Leaked personal information details

Name of the individual with whom the contract is made, email address, the name of a corporation, affiliated department/position, address (personal), the date of birth, telephone number (corporation/individual), nationality, gender, face photo, etc., passport number, biography, bank account, driver's license number

◆The number of individuals whose personal information was leaked
The number of individuals as customers whose personal information was leaked was 94.

(2) Business partners similar to our customers other than our customers as a financial instruments business operator
①: Although business partners are not our customers as described above, they are similar to our customers who were investigated this time as investors of our funds.

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 135.

②: Related parties that were investigated this time as our business partners who did not apply to ① are described below.
②-1: Business partners with whom we are a customer under financial instruments trading contracts

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 36.

②-2: Business partners and their relevant parties to whom our Company, which is other than ②-1, is a customer of financial instruments trading contracts and to whom we are entrusted with business operations.

◆Leaked personal information details
The name of an individual, email address, the name of a corporation, affiliated department/position, address, telephone number, the name of the individual's family, the date of birth (other than the individual), telephone number (other than the individual), relationship, address (other than the individual).

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 48.

(3) Personal information of the following parties was leaked: Relevant parties and business partners other than (1) our customers with whom we have contracts under the Financial Instruments and Exchange Act, such as related parties and business partners excluding our customers and business partners similar to our customers; and (2) business partners similar to our customers other than our customers. Details of the affected parties are described below.

③-1: Business partners with whom we have contracts involved in the management of the fund or Customers of the fund, etc. (securities companies, administrators, law firms, and other parties involved in the management of the fund).

◆Leaked personal information details

The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, the accountant license number, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 689.

③-2: Potential investors, competitors, invested companies, people involved with invested companies, etc.

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, passport number, address, age, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 1,103.

③-3: Vendors that we use including merchandisers, information vendors, staffing agencies, etc.

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, address, bank account, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 178.

③-4: Domain of providers, acquaintances, job applicants, etc.

◆Leaked personal information details
Name, email address, the name of a corporation, affiliated department/position, telephone number, etc.
For job applicants, gender, address, telephone number, the date of birth, age, biography, face photo, hobby

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 148.

③-5: Others (Those who cannot be categorized as above)
Although individuals belong to none of the categories mentioned above, they have operational ties with our Company or the outsourcing companies that handle our Company's operations.

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, telephone number, biography, photo, etc.

◆The number of individuals whose personal information was leaked
The number of individuals whose personal information was leaked was 47.

③-6: Supervisory agencies, administrative agencies, associations, etc.

◆Leaked personal information details
The name of a person in charge, email address, the name of a corporation, affiliated department/position, address, etc.

◆The number of individuals whose personal information was leaked

The number of individuals whose personal information was leaked was 62.

3. Cause of the information leak
The cause was that our security measures were in a vulnerable state due to the fact that passwords were not being changed regularly and that we were considering introducing two-step verification but had not done so.

As a possible cause of the leak, the forensics investigation pointed out that the password that the Affected Employee registered on an external website might have been leaked. The cause of the password leak could not be determined.

4. Secondary damage or whether there is a possible secondary damage and its details
According to our internal investigation, it was confirmed that the file attached to spam emails did not contain some kind of virus and was not ransomware or malware, because it was possible to open the file. (The confirmation is limited to the virus test conducted on the user's PC that was opened by us.)

Please be careful if you receive a suspicious email, because emails soliciting investments may be sent by a third-party who uses leaked email addresses or personal information.

5. Implementation status of response measures for individuals whose personal information was leaked
We explained the situation to our customers right after the incident occurred. As we made a final report this time, we once again explained to our customers about personal information details that were leaked.

6. Implementation status on disclosure
We issued our first press release on May 31, 2024, and the second one on June 14, 2024. This will be our final report.

7. Measures to prevent recurrence
As preventative steps, we implemented the following measures.
① Change passwords regularly: We change passwords once every three months to eliminate vulnerabilities in our security measures, which became the cause of this incident.

② Introduction of two-factor authentication: In addition to regular authentication using IDs and passwords, all our officers and employees took measures to prevent identity theft by adding another step to verify their identities. (Those who are concurrently employed at other companies will follow the regulations of the company to which they belong.)

③ Prohibition on using the same password: In the forensics investigation, it noted the possibility that authentication information registered on an external website might have been leaked. We alerted all officers and employees about prohibition on using the same password.

④ Enhancing literacy on personal information and cybersecurity: We strive to improve literacy on personal information and cybersecurity through training with our group company AIZAWA SECURITIES CO., LTD..

8. Other matters for reference
In addition to personal information of nine of our company's officers and employees (including those who retired) and their dependents had their specific personal information leaked, and this was reported to the Personal Information Protection Commission on July 10, 2024.

<Contact for inquiries regarding this matter>
Aizawa Asset Management Co., Ltd.
Client Solutions Department
TEL: 03-6263-9690

MAIL: clientsolutions@aizawa-am.co.jp