March 31, 2023

To Whom It May Concern,

Company name Adastria Co., Ltd.
Representative Osamu Kimura, Representative Director and President
(Securities code: 2685 TSE Prime Market)
Inquiries Itsuo Iwakoshi, Senior Executive Officer, Executive General Manager of Administration Division and Head of Corporate Planning Office
(TEL:03-5466-2060)

# Regarding Unauthorized Access to Company Servers (follow-up report)

As announced on January 19 and 24, 2023 (“Previous Reports” *1, *2, below), we must, unfortunately, recognize the possibility that certain customer personal information may have been leaked in connection with unauthorized access to our servers (the “Incident,” below).
Now that a forensic investigation (*3) by an external specialized agency and internal investigation have concluded, we will report the results of the investigation and measures to prevent recurrence.

The company’s systems have been restored, and there has been no leakage of information related to this matter extending from the time of the discovery of the Incident to the present. The information for which leakage was possible did not include credit card and other payment information, nor did it include Individual Numbers.

We apologize sincerely for any inconvenience and concern this may cause our customers and other related parties.

*1 See *Regarding Unauthorized Access to Company Servers* (Japanese only)
https://www.adastria.co.jp/news/notice/entry-15640/
*2 *Notice and Apology Concerning Possible Leakage of Customer Personal Information*
https://www.adastria.co.jp/english/news/ir/entry-15642/
*3 Forensic investigation: A forensic investigation is an investigation that extracts evidentiary data from the storage on digital devices. Activity records serving as evidence of illegal activities are identified from within communication records stored on servers and communication devices.

## 1. Events Leading to the Incident

Early on the morning of January 18, 2023, we confirmed that certain internal business system servers, etc., ("Servers", below) had been accessed illegally by an outside third party. Immediately after confirming the Incident, we took measures to prevent the spread of damage, including shutting down our network and our internal business systems. We established a task force later on the morning of the same day. With the cooperation of specialized outside agencies, we began to identify the extent of the impact related to this Incident. We investigated the cause and intrusion route, and began restoration work, etc. We submitted a report on this matter to the Personal Information Protection Commission and to the police.

The following is a summary of actions taken subsequently.

・January 19, 2023 (Thursday) Issued a public announcement (first report)
・January 20, 2023 (Friday) through February 17, 2023 (Friday)　Launch of investigation by digital forensic experts to investigate the underlying cause of the Incident
・January 24, 2023 (Tuesday) Issued a public announcement (second report)
・February 20, 2023 (Monday) Received the results of the forensic investigation from the external professional organization
・February 20, 2023 (Monday) through March 20, 2023 (Monday) Continued with internal investigation based on forensic investigation results
・March 20, 2023 (Monday) Submitted a report to the Personal Information Protection Commission
・March 31, 2023 (Friday) Issued a public announcement (third report)

2.　Facts Revealed by the Forensic Investigation and Internal Investigation

・Identified intrusion route by outside third party
・Identified devices affected by unauthorized access
・Identified the scope of information that may have been leaked

3.　Potential Information Leakage

The following is a list of information newly identified since the previous report as having potentially leaked.

Payment information, including credit card information, and Individual Number information was not included in the leakage. We have not confirmed the actual leakage of customer information related to the Incident at this time.

・**Certain customer information obtained via telephone inquiries to customer service between 2008 and 2013**
(Name, summary of inquiry, etc.) 221,272 records
・**Employee information (including retired employees) for individuals been employed by the Group (*4) since 2008**
(Name, address, date of birth, personnel information, etc.) 94,435 records
・**Information for certain applicants who participated in new graduate recruitment in 2018 or later**
(Name, telephone number, e-mail address, etc.) 22,063 records
・**Information for certain applicants who participated in mid-career and part-time recruiting in 2005 and later**

(Name, telephone number, e-mail addresses, etc.) 26,460 records

・**Information for certain business partners**

(Name, company e-mail address, etc.) 6,346 records

*4 Excludes zetton inc. and OPEN AND NATURAL Inc.

To the greatest extent possible, we will send individual notices to affected individuals by e-mail or regular mail. As we do not have contact information for many individuals, we established the following telephone number for inquiries.

[Customer Inquiries]

・Toll-free number: 0120-497-585 (Hours: 10:00-19:00, including Saturdays, Sundays, and national holidays)

Inquiry form: https://support.adastria.co.jp/hc/ja/requests/new

*Due to the high volume of calls, it may be difficult to contact a representative. If you are unable to reach us, please try again later. We apologize for the inconvenience.

4. Measures to Prevent Recurrence

We implemented the following measures based on the results of the investigation.

・We terminated the use of affected devices and devices that may have been affected

・We reset various accounts, and we reviewed and strengthened management policies

・We now use the latest security products to search for breaches, continuing to investigate and monitor suspicious processes on devices, protect devices, etc.

We also confirmed no traces of unauthorized access and hardened security measures, even for devices not found to have been compromised. Hardened measures included full scans with the latest security software, stronger account password policies, and enhancing monitoring of end-point terminals. We will continue to work with external specialists to ensure the security of our operations.

Adastria is committed to further enhancements to security and monitoring systems in cooperation with external specialized agencies to prevent recurrence.

5. Impact on Business Performance

At this time, we have made no changes to earnings forecasts or other matters related to this incident. The company will promptly disclose any matters that arise in the future that require disclosure.

We apologize sincerely for any inconvenience and concern this matter may have caused our customers and other related parties.

Contact Information

[Customer Inquiries]

・Toll-free number: 0120-497-585

(Hours: 10:00-19:00, including Saturdays, Sundays, and national holidays)

・Contact Form:

https://support.adastria.co.jp/hc/ja/requests/new

[Media Inquiries]

・Adastria Public Relations Department

03-5466-2050