

Allen Overy Shearman Sterling US LLP

599 Lexington Avenue

New York, NY 10022

Tel: +1.212.756.1157

andrew.tannenbaum@allenovery.com

Anthony G. Brown

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

RE: Notice of Data Breach

Dear Mr. Brown,

We are writing on behalf of our client, H2O.ai (“H2O”). H2O was recently the target of a cyber event that impacted a limited part of its environment. We are providing notice because the impacted environment contained personal information pertaining to H2O current and former employees, including twelve residents of Maryland.

On February 18, 2025, we became aware that a financially motivated threat actor claimed to have stolen H2O data. We quickly retained leading cybersecurity firms to assist in responding to this claim and to help conduct an investigation. The investigation revealed that a threat actor accessed certain H2O systems at various times between December 20, 2024, and January 29, 2025. During the course of our investigation, H2O became aware that personal information, including data belonging to H2O current and former employees, had been accessed and may have been exfiltrated by the unauthorized actor.

The affected information was identified in a limited number of payroll and employee-related files stored in the affected environment. These files contained payroll and compensation information, 401k contribution information, social security numbers, driver’s license numbers, address information, and dates of birth. Indeed, the majority of the impact was to internal H2O.ai data such as our business, sales, and financial materials, as well as customer agreements and purchase orders.

We have no indication that the unauthorized actor was targeting personal data and no evidence that personal information has been or will be misused to cause any harm to individuals as a result of this incident. Nonetheless, in an abundance of caution, we are providing notice to all current and former employees. A copy of that notice has been submitted in connection with this filing.

Please be assured, we immediately reported the incident to law enforcement. To prevent a similar occurrence, we implemented measures to enhance the security of our network systems and data. These include:

- Reviewing our security controls, including segmentation between our environments.

- Taking the impacted environment offline.
- Implementing enhanced monitoring to detect and mitigate threats in real-time.

We will continue to evaluate additional steps that may further protect H2O's security.

Sincerely,

Andrew Tannenbaum



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 27, 2025



N1069-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

A standard 1D barcode representing the alphanumeric string N1069-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345. The barcode consists of vertical black bars of varying widths on a white background.

RE: Notice of Data Breach

Dear Sample A. Sample:

H2O.ai (“H2O”) was recently the target of a cyber event that impacted a limited part of our environment. Because the impacted environment contained personal information pertaining to H2O current and former employees, we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on proactive steps you may consider taking to help protect your information.

What Happened?

On February 18, 2025, we became aware that a financially motivated group claimed to have stolen H2O data. We quickly retained leading cybersecurity firms to assist in responding to this claim and to help conduct an investigation of the incident. The investigation revealed that an unauthorized actor accessed certain H2O systems at various times between December 20, 2024, and January 29, 2025. During the course of our investigation, H2O became aware that personal information, including data belonging to H2O employees, had been accessed and may have been exfiltrated by the unauthorized actor. We have no indication that the unauthorized actor was targeting your data and no evidence that your information has been or will be misused as a result of this incident.

What Information Was Involved?

As part of its investigation, H2O found certain information pertaining to you in payroll files, billing information, 401k contribution statements, earnings statements and tax forms. This information included your name and one or more of the following: payroll information, Social Security Number, driver's license number, home address, date of birth, and benefit enrollment information.

What Are We Doing?

We immediately reported the incident to law enforcement and continue to cooperate with their investigation. To prevent a similar occurrence, we implemented numerous measures to enhance the security of our network systems and data. We will continue to evaluate additional steps that may further protect H2O's security.

What Can You Do?

Please review the “Information About Identity Theft Protection” reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or security freeze on your credit file.

To help you protect your identity, we are offering complimentary access to Experian IdentityWorksSM. for ## months.

ENGAGE#

0000001



N1069-L01

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** June 30, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-3956 by June 30, 2025. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information.

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please call 1-833-918-3956, Monday through Friday between 6 a.m. to 6 p.m. Pacific (excluding major US holidays). Please be prepared to reference ENGAGE# when speaking with an agent.

Sincerely,
SriSatish Ambati

CEO | H2O.ai

people@h2o.ai

ENGAGE#

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies — Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to vwww.consumerfinance.gov/learn-more or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.



Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-8085318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, (410) 528-8662.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>; and the Consumer Frauds & Protection Bureau, 120 Broadway 3rd Floor, New York, NY 10271 (800) 771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400. You may also file a police report by contacting local or state law enforcement agencies. You have the right to file or obtain a police report regarding this incident.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General. You may contact the Iowa Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5926, (888) 777-4590.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General, Oregon Department of Justice, 1162 Court Street NE Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.