CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

February 24, 2021

Via Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Breach Notification

To Whom It May Concern:

We are writing on behalf of our client, Aduro, LLC ("Aduro"). Aduro hosts an employee wellness program on behalf of employers, many of whom constitute covered entities subject to the Health Insurance Portability and Accountability Act ("HIPAA"). The security incident concerns Limeade, Inc. ("Limeade"), a third-party technology provider utilized by Aduro to support its program offerings.

On December 21, 2020, Aduro was advised by Limeade that a number of participants of the Aduro-serviced well-being program were impacted by a credential stuffing attack whereby an unknown actor was able to use automated credential-guessing programs to gain access to participant accounts hosted on the Limeade system. Upon discovering this incident, Limeade advised Aduro that it conducted a thorough forensic investigation and determined that the attack's goal was to access user accounts for the sole purpose of leveling up participant points within the wellness program to then divert gift cards to their own email accounts.

Following Limeade's initial notification of the incident, Aduro immediately requested Limeade provide all information regarding the incident's full nature and scope and promptly notified its employer-customers. Through thorough investigation, Limeade determined that the unauthorized access may have allowed access to individuals' names, email addresses, account credentials, and in a small number of instances dates of birth and/or certain biometric information. These individuals are associated with the employers and/or covered entities whom Aduro services. Since the time of Limeade's initial notification of this incident, Aduro has worked diligently to keep the employers and covered entities reasonably informed.

In response to this incident, Limeade has indicated that they have taken steps to further secure their environment through various measures, including revised email change processes,

forced password resets, added data security protocols, and the future implementation of multi-factor authentication to further improve its security platform.

At this time, Aduro is aware of one (1) New Hampshire resident who may have been affected and will require notification. As the investigation remains ongoing, we will provide supplemental notification should we determine additional New Hampshire residents were affected.

As a courtesy, Aduro notified all affected individuals by email earlier this month. Aduro has been working with its employer-customers to obtain postal addresses for each affected individual and, beginning on February 24, 021, Aduro will also mail notification letters via United States Postal Service First Class mail to affected individuals. We will provide these individuals with one (1) year of complimentary identity monitoring services, including one (1) year of credit monitoring. A sample copy of the notification letter is attached, which outlines the incident and provides affected individuals with additional resources to protect their identity and monitor their credit history and personal accounts. Aduro is taking all steps to comply with all applicable notification obligations.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: NOTICE OF DATA BREACH

Important Security Notification. Please read this entire letter.

Dear <<Name 1>>:

Our records indicate that you or your spouse/partner is enrolled in an employee wellness program hosted by Aduro, LLC ("Aduro"). Aduro uses a technology provider, Limeade, Inc., to provide certain technology services that support their offering. Aduro is writing to inform you of a data security incident experienced by Limeade wherein some of your personal information was compromised (limited to your first and last name, email address, account password, and, *only if you had entered it in the platform,* date of birth).

We are writing to inform you of this incident, to offer information about steps that can be taken to help protect your information and to let you know about complimentary credit monitoring services that are being offered to you.

Credit Monitoring:

In an abundance of caution and to help relieve concerns, we have secured the services of Epiq to provide TransUnion's myTrueIdentity identity monitoring at no cost to you for one year. Epiq is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of personal information. To obtain a unique activation code to enroll in the credit monitoring service and instructions on how to do so, please email incidentresponse@adurolife.com. Note that, because an individual activation code will be generated specifically for you, it may be a few business days from receipt of your email before a code will be emailed back to you.

What Happened:

On December 21, 2020, we were advised by Limeade that a number of participants of the Aduro-serviced well-being program were impacted by a credential stuffing attack whereby an unknown actor was able to use automated credential guessing-programs to gain access to participant accounts hosted on the Limeade system. Upon discovering this incident, Limeade conducted a thorough forensic investigation and determined that the goal of the attack was to access user accounts for the sole purpose of leveling up participant points to then divert gift cards to their own email accounts.

Following Limeade's notification of this incident to Aduro, we immediately requested that Limeade provide additional information to Aduro regarding the full nature and scope of the incident.

What Information Was Involved:

According to Limeade and their forensic experts, the goal of this incident was to access user accounts for the sole purpose of leveling up participant points to then divert gift cards to their own email accounts. Limeade, however, cannot rule out that certain of your personal information may have been accessible including your first and last name, email address, account password, and, if you entered the information into the platform yourself, your date of birth. According to Limeade, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Nevertheless, out of an abundance of caution, we wanted to advise of this incident and provide you with resources to protect your information.

What Is Being Done:

Limeade has indicated that they have taken steps to further secure their environment through various measures, including revised email change processes, password updates, and additional security monitoring. Eventually, they plan to implement "multi-factor authentication" to further improve platform security.

What You Can Do:

No financial information or sensitive information, such as your social security number, was compromised. Aduro recommends that you remain vigilant in regularly reviewing and monitoring all of your financial account statements and obtaining copies of your credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly follow up with the applicable financial institution or company. There are procedures available to contest fraudulent charges or errors on your credit report that are the result of identity theft. Additionally, we recommend that you regularly change any passwords or other security account credentials across all platforms including any Aduro account credentials. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact incidentresponse@adurolife.com. The security of our participants' personal information is of the utmost importance to us and we deeply regret this incident.

We remain committed to protecting your trust in us and continue to be thankful for your engagement with Aduro as the provider behind your employee wellness program. Please accept our regrets for any worry or inconvenience that this Limeade incident may cause you.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

- **PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834
1-800-680-8289
www.transunion.com

Experian
National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements.

Be proactive and create alerts on credit cards and bank accounts to notify you of activity.

If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

  You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.

- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

- **For New York residents,** you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.