

# evidation

23474

## NOTICE OF INCIDENT

Dear Achiever,

We value and respect the privacy and security of your information, which is why we are writing to let you know about an incident which occurred between September 15th and September 30th, 2021, involving suspicious activity in your Achievement account. We are providing notice to you and other potentially affected customers about the incident, and also providing information about tools and resources available to you to protect yourself online as well as to prevent any potential fraud or identity theft.

Based on our review of the suspicious account activity, it is likely that the attacker(s) had access to any information you supplied to us that would be viewable to you in your Achievement account. However, to date, we have not uncovered anything that would lead us to believe that our own Achievement app or systems have been compromised. We are providing you with notice for your awareness and so you can take steps to secure your Achievement and other online accounts.

### What We Are Doing

To contain the suspicious activity, we have temporarily deactivated your account. To reactivate your account, you will need to contact Customer Service by emailing [help@myachievement.com](mailto:help@myachievement.com) or by replying directly to this message. When you reach out to reactivate your account, our Customer Service representatives will ask you for information to help us verify your account.

Because we know you worked hard to earn points on Achievement and have contributed to public health and research initiatives during your time on our platform, upon reactivation of your account we will reinstate any Achievement points you may have lost as a result of this activity.

We value your privacy and deeply regret that this incident occurred. We will continue to review this incident and will notify you if there are any significant developments. Although this incident did not result from a breach or vulnerability of the Achievement app or systems, we wanted to inform you of this incident as we value the privacy and security of your account and information.

In addition to notifying you of this incident, we also wanted to provide you with resources and information you can use to further protect your online presence both on Achievement and beyond, including to guard against identity theft or fraud.

### What You Can Do

EVIDATION HEALTH, INC.  
63 Bovet Rd. #146  
SAN MATEO, CA 94402

# evidation

*File a police report.* Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

*Update your credentials.* To prevent suspicious activity occurring in any other online accounts, you should update your credentials and review any activity on those accounts. Be sure to report any suspicious activity to that account or app.

*Monitor your accounts.* If you use the same or similar credentials on any financial, banking, credit, or budgeting accounts or apps, you should review your activity on those accounts, including any credit and debit card account statements, as soon as possible to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your accounts and any statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have already taken place, you should contact the company or app immediately to report that activity.

*Check your credit and place a fraud alert or freeze on your accounts.* You should also carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, please reach out to your local law enforcement office and credit agency.

*Additional resources and information.* Also, please review the below "Information about Identity Theft Protection" that describes additional steps you may take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection, and additional details on how to place a fraud alert or a security freeze on your credit file.

## **For More Information Or If You Have Any Questions**

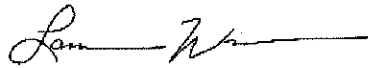
Once again, we are sorry that this incident occurred. If there is anything else that we can do to assist you, or if you have any questions about this notice, please reach out to our Privacy team at:

Achievement  
Attn: Privacy  
63 Bovet Rd #146  
San Mateo, CA 94402  
[privacy@myachievement.com](mailto:privacy@myachievement.com)

# evidation

You can also refer to the Achievement Privacy Policy for additional information as well as your privacy rights. The Policy is available at <https://www.myachievement.com/privacy> and on the Achievement app.

Sincerely,

A handwritten signature in black ink, appearing to read "Lauren Wu", with a long horizontal flourish extending to the right.

Lauren Wu  
Head of Privacy at Evidation Health

# evidation

***The following information has been provided by the Federal Trade Commission (FTC) as a resource for all consumers. Evidation Health has not prepared these materials, but only compiled them for your convenience.***

***We have also included additional information specific to Massachusetts below.***

-----

## **From the FTC: Information about Identity Theft Protection**

**Fraud Alert:** The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

**Equifax:** [equifax.com/personal/credit-report-services](http://equifax.com/personal/credit-report-services)(link is external) or 1-800-685-1111

**Experian:** [experian.com/help](http://experian.com/help)(link is external) or 1-888-397-3742

**TransUnion:** [transunion.com/credit-help](http://transunion.com/credit-help)  
or(link is external) 1-888-909-8872

**Get & Review Your Credit Report:** Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. You may also obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. These can be signs of identity theft.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC.

# evidation

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly. In fact, the FTC recommends that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

**Report Any Suspicious Activity:** If your personal information has been misused, report the identity theft and get recovery steps. You may contact the FTC or your state's regulatory authority to report any fraudulent activity, and obtain additional information about avoiding and protection against identity theft:

*Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).*

You should also call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

**Credit Freeze (also known as a Security Freeze):** You may also want to consider placing a free credit freeze on your accounts. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

-----  
***You may also obtain information about preventing and avoiding identity theft from, as well as reporting suspected incidents of identity theft to your Attorney General, in addition to your local law enforcement office. Please see below for more information.***

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Under federal law, you cannot be charged to place, lift, or remove a security freeze.

# evidation

You must place your request for a freeze with each of the three major consumer reporting agencies:

Equifax ([www.equifax.com](http://www.equifax.com));  
Experian ([www.experian.com](http://www.experian.com)); and  
TransUnion ([www.transunion.com](http://www.transunion.com)).

To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-349-9960  
<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
<https://www.transunion.com/credit-freeze>

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;

# evidation

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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.