

# evidation

## 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 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.

### **What Happened?**

We first became aware on September 16, 2021, of suspicious redemptions on your account through our point redemption vendor, Tremendous. After becoming aware of this activity, we initiated an investigation to uncover how this access occurred, and took steps to stop any suspicious activity and secure your account.

Based on our investigation, we have determined that one or more third parties gained access to an email or username and password (known as your credentials) that you may have used for another service or app, and used those credentials to access your Achievement account. This is known as a “credential stuffing attack.” Our investigation indicates that the suspicious activity on Achievement occurred on or around September 15th, 2021 and continued through September 18th, 2021. We are unable to determine when and how these third parties may have gained access to your credentials.

To date, we have not uncovered anything that would lead us to believe that our 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 Information Was Involved?**

Because your login credentials were used to access your account, 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. This information may include your first name and last name, phone number, mailing address, gender, birthday, and race/ethnicity (each, only if provided). It is possible that these third parties may also have viewed information about the surveys you’ve taken (not your responses), your points, and any other documents stored with your profile and accessible with login credentials. We are unable to confirm what specific information, if any, was actually accessed by these third parties.

# evidation

We are aware that these third parties may also have attempted to change the email used to redeem your Achievement points and tried to initiate point redemption. In some cases, we were able to prevent any redemption activity. However, we understand from Tremendous that some redemptions may have been completed by these third parties.

## **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). 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. We have taken a number of steps to try to prevent further activity from these malicious third parties and recurrence of a similar attack. 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**

*Update your credentials.* Because these malicious third party actors had access to your account credentials, it is likely that they can access any online accounts where you use the same or similar credentials. To prevent similar activity occurring in these other 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

# evidation

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 details on how to place a fraud alert or a security freeze on your credit file.

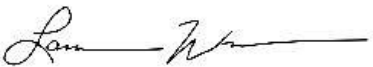
## **For More Information or if you have any Questions**

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)

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,



Lauren Wu  
Head of Privacy at Evidation Health

## Additional Information from the Federal Trade Commission

*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 included additional information specific to residents of the State of Maine, as provided by the Office of the Attorney General.*

### 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.

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.

## Additional Information from the Federal Trade Commission

**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:** 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.

**From the Office of the Attorney General of Maine**

## Privacy, Identity Theft and Data Security Breaches

Today's technology provides us with extraordinary benefits. It has given us the ability to conduct business online, share information about ourselves with those who live thousands of miles away and access information at the "speed of light." Unfortunately, it has also provided the same benefits to identity thieves who use someone else's personal financial information to access bank accounts and obtain credit, often destroying the life savings and good credit history of innocent victims.

As our access to information increases, our concerns about financial privacy should increase as well. Identity theft has increased so dramatically that the Federal Trade Commission has listed it as the top fraud-related consumer complaint for the past five years, with consumers reporting million of dollars lost to fraud. Millions of people are potentially at risk for identity theft. The following is provided to help you protect your financial privacy and the steps to follow if you have become an identity theft victim.

### Identity Theft

Everyone has personal information (such as credit card numbers, bank account numbers, and social security numbers) that can be misused when in the wrong hands. A scam artist who learns any of your personal information can potentially use that to learn more of your personal information and eventually make purchases in your name.

[Learn how to protect yourself from identity theft](https://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml)

([https://www.maine.gov/ag/consumer/identity\\_theft/identity\\_theft.shtml](https://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml)).

### What to do if you're a victim of Identity Theft

Identity theft is a crime which generally results in fraud. If you believe you have become a victim of identity theft, you must act immediately to minimize the damage and to secure your legal rights. Fighting identity theft can be frustrating and time-consuming, but [resources exist to help you](https://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml)

([https://www.maine.gov/ag/consumer/identity\\_theft/identity\\_theft.shtml](https://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml)).

## Additional Information from the Federal Trade Commission

# Common Consumer Scams

### Scams: Keep These Tips in Mind

As a general rule, all scams have similar traits. Here are some obvious ones that raise red flags in the Consumer Protection Division that you should keep in mind.

You are contacted out of the blue. Anyone who calls, emails, send you a letter, texts or comes to your dooryard out of the blue may not have your best interest at heart. You don't have to respond right away, make a decision or even answer the door.

You have to send money up front in order to receive a prize. You haven't won anything if you have to pay for it.

You need to send money via wire transfer or a reloadable card. This is frequently the preferred way for scammers to ask for money. Remember, this is just like sending someone cash - you'll never see it again.

You are asked for personal or financial information. Never provide your personal information (DOB, SSN, etc.) or bank account information to someone you don't know. Your bank or credit card company will not call and ask to confirm any account or personal details they already have on file. Anyone asking for this information out of the blue is trying to scam you.

Don't tell anyone. Scammers want to keep you under their spell. If you tell family and friends, someone may ask dissuade you from interacting with them. If you're asked to keep it a secret, it is a scam.

ACT NOW! If an offer is really good, it can wait for you to sleep on it and get back to them tomorrow. Too many times though, scams have to be acted on today only. We advise you to be slow to say yes and quick to say no.

You get a real looking check. If you get a check and are asked to send money back, it's a scam. If you really think you've come upon unexpected good fortune, take your check to the bank and ask them to verify whether it is real.

Always listen to your gut. If it sounds too good to be true, it is.