

SENT VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
[Email:ldtheft@oag.state.md.us](mailto:ldtheft@oag.state.md.us)

NOTICE OF INCIDENT

We are providing notice to your office of a recent security incident affecting our platform, known to users as the Achievement mobile application.

What Happened?

We first became aware on April 14, 2022, of suspicious activity through our customer support team.

Our internal investigation determined that ~ one (1) Maryland resident was likely the target of a credential stuffing attack, i.e., one or more third parties harvested these users' login credentials (email or username and password) from another service or app and then used these credentials to access this users accounts on our platform. The suspicious activity occurred on or around February 8th, 2022 and continued through April 14th, 2022. We are unable to determine when and how these third parties may have gained access to the credentials.

To date, we have not uncovered anything that would lead us to believe that our app or systems have been compromised.

What Information Was Involved?

Because login credentials were used for access, it is likely that the attacker(s) had access to any information supplied in the user's account, which could include first name and last name, phone number, mailing address, gender, birthday, and race/ethnicity (each, only if provided), the fact that the user took surveys (though not the user's survey responses), points in the user's account, and any other documents stored with the user's profile. We are unable to confirm what information, if any, was actually accessed by these third parties.

In this case, we are aware that these third parties changed the email associated with the account and attempted to initiate point redemption.

What We Are Doing

We have temporarily deactivated the affected account and are requesting the user contact Customer Service to reactivate the account, which will require the user to go through our account verification process, including a mandated password reset.

Though this incident does not appear to have resulted from a breach or vulnerability of our app or systems, we have taken a number of steps to try to prevent further activity from these malicious third parties and recurrence of a similar attack, and will continue to review our processes and procedures for other areas where we can enhance our existing controls.

Following our notice to you, we will be providing the affected Maryland resident user with additional information and resources from the FTC and general contact information for your office (the Office of the Attorney General) to further protect their online presence, including to guard against identity theft or fraud.

Also included is a copy of the notice which will be sent to Maryland user, attached below.

For More Information

Below is our contact information in the event of further questions:

Evidation
Attn: Privacy
63 Bovet Rd #146
San Mateo, CA 94402
privacy@myachievement.com

(650) 897-5968

Respectfully,
Lauren Wu
Head of Privacy at Evidation

NOTICE OF INCIDENT

Dear Achiever,

We value and respect the privacy and security of your information, which is why we are writing to respond to your inquiry and let you know about an incident involving suspicious activity in your Evidation account. We are providing notice to you about the incident, and also providing information about tools and resources available to you to protect yourself online.

What Happened?

We first became aware of suspicious redemptions on your account based on your inquiry to us in April 2022. Thereafter, we initiated an investigation to uncover how this activity occurred, and took steps to stop any further 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 Evidation account. This is known as a “credential stuffing attack.” Our investigation indicates that suspicious activity in your Evidation account began on February 8, 2022 and occurred most recently on February 14, 2022. Your account was deactivated for your protection on April 14th, 2022, the date on which our team at Evidation reviewed your email. We are unable to determine when and how these third parties may have gained access to your credentials. On February 8, a third party submitted a support ticket to our customer service team requesting we change the email associated with the account. This change was made by the customer service representative because this person was able to provide us the correct answers to our verification questions. We did not become aware that you, as the account holder, had not made this request until you contacted us. Your account was deactivated once we became aware of the suspicious activity.

To date, we have not uncovered anything that would lead us to believe that our Evidation app or systems have been compromised. We are providing you with notice for your awareness and so you can take steps to secure your Evidation 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 Evidation 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 within your profile and accessible with login credentials. We are unable to confirm what specific information, if any, was actually accessed by these third parties.

What We Are Doing

To contain the suspicious activity, we deactivated your account in order to prevent any further access while we investigated this occurrence.

At this time we have reverted the unauthorized account email back to the original email address associated with your account and pushed a password reset notification to this email. Your account has since been reactivated and you will be able to access it after completing a password reset.

You should have received another email with instructions on how to update your password. Please follow the steps to create a new password. If you are attempting to reset your password on your mobile device and are unsuccessful, please try using your laptop/computer and sign on at www.my.evidation.com.

Because we know you worked hard to earn points on Evidation and have contributed to public health and research initiatives during your time on our platform, upon reactivation of your account we will reinstate any Evidation 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 Evidation app or systems, we want 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 want to provide you with resources and information you can use to further protect your online presence both on Evidation 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, please 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. Please 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, please contact the company or app immediately to report that activity.

Check your credit and place a fraud alert or freeze on your accounts. Please 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:

Evidation
Attn: Privacy
63 Bovet Rd #146
San Mateo, CA 94402
privacy@evidation.com

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

Sincerely,



Lauren Wu
Head of Privacy at Evidation Health

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 Maryland provided 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(link is external) or 1-800-685-1111

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

TransUnion: 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, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at 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.

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.

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 state's Attorney General, in addition to your local law enforcement office. Below is the contact information for Maryland's Office of the Attorney General.

Maryland Office of the Attorney General – Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us