

May 23, 2025



00695-ADFFIN L001 AUTO *000001

To [REDACTED],

HealthEquity, Inc. (HealthEquity) is writing to let you know about a data security incident. HealthEquity manages health financial accounts such as FSAs and HRAs on behalf of employers and/or insurance companies, including Mass Bankers Association. This data security incident resulted in unauthorized access to or disclosure of some individuals' personal health information (PHI) including yours or your dependent's. We are not aware of any actual or attempted misuse of information because of this incident to date.

What happened?

On September 19, 2024, HealthEquity's security protocols detected a high volume of unauthorized attempts to access certain member accounts, activating alerts. Upon further investigation, HealthEquity discovered it was the target of a credential stuffing attack aimed at stealing members' funds. Credential stuffing is a type of cyberattack that uses automated tools to input large volumes of stolen username and password combinations into a website's login page to gain unauthorized access to accounts. These credentials are often obtained from other data breaches and are publicly available or sold on the dark web.

HealthEquity disabled access to the affected accounts and began a forensic investigation to determine the full scope of the incident. The attack was driven by financial motives. On March 13, 2025, HealthEquity determined that your information was impacted by this attack.

What information may have been involved?

Our investigation found that the following information related to you may have been subjected to unauthorized access during this incident:

- Your name
- Your provider's names and demographics
- General claims information, including dates of service
- Amount of funds available and/or amount paid

What are we doing?

Once we detected the suspicious activity, we immediately launched an investigation and engaged third-party experts to determine the nature and scope of the incident. As a result of our investigation, we have enhanced our security and monitoring efforts, internal controls, and security posture. Some notable enhancements include enacting a global password check on accounts and integrating multiple layers of identity validation. We also reimbursed any members' accounts whose funds were impacted.



What can you do?

Because of the impact this might have on you, HealthEquity has arranged credit identity monitoring services for a period of **two years, free of charge**, through Equifax **326142644994**. You have until August 31, 2025 to activate these services. Instructions on how to activate your free Equifax monitoring subscription are included in the enclosed Reference Guide.

The Reference Guide also includes information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review financial statements, credit reports and other accounts to ensure that all account activity is valid.

For more information

If you have any questions or would like additional information, please refer to the enclosed Reference Guide, or call toll-free **1-855-260-8354**. This service center is open from 8:00am – 8:00pm CT, Monday through Friday, excluding some U.S. holidays.

We sincerely regret that this incident occurred. HealthEquity takes the security of personal information seriously, and we will continue to work diligently to protect the information entrusted to us.

Sincerely,

A handwritten signature in black ink, appearing to read 'Michael Fiore', with a stylized, cursive script.

Michael Fiore

Executive Vice President and Chief Commercial Officer

Reference Guide – Equifax

Because of the impact this might have on you and your dependents, HealthEquity has arranged credit identity monitoring, insurance, and restoration services for a period of two years, free of charge, through Equifax. Use your unique activation code **326142644994** to enroll online at **www.equifax.com/activate**. You have until August 31, 2025 to activate these services.

Review Your Account Statements

Carefully review statements sent to you from HealthEquity to ensure that your account activity is correct. Report any questionable charges promptly.

Confirm Personal and Contact Information on the HealthEquity Portal

Log on to the HealthEquity portal and confirm that your personal profile and contact information are correct.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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



Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report, you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax	P.O. Box 105069 Atlanta, GA 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than one business day after receiving a request by phone or secure electronic means, and no later than three business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Massachusetts

You have the right to obtain a police report with respect 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.

For Residents of the District of Columbia

You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft:

D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, 1-202-442-9828, www.oag.dc.gov

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

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 place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.



A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us

For Residents of Rhode Island

You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov