Version A

HealthEquity

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017-4044

To enroll, please call:
(877) 916-8380
Or Visit:
https://ide.myidcare.com/healthequityprotect
Enrollment code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 15, 2018

Dear <<First Name>> <<Last Name>>,

NOTICE OF DATA BREACH

We are writing to inform you of a data security incident that involves your personal information. On October 20, 2018, HealthEquity began receiving the results of analysis confirming that a cyberattack on HealthEquity may have exposed sensitive personal information for certain individuals. You are receiving this letter because some of your personal information was found in this analysis.

What happened
On October 5, HealthEquity's information security team identified unauthorized logins to two HealthEquity team members' email accounts. We immediately implemented security measures to prevent further access to the accounts, and began analyzing all information contained in these accounts to identify any sensitive personal information. The unauthorized access occurred, in the case of one account, on October 5, and in the case of the other, on different occasions between September 4, 2018 and October 3, 2018.

What information was involved
The email accounts contained documents that included personal information that is used by HealthEquity to manage member accounts. The affected HealthEquity employees' email accounts had these materials for legitimate business purposes. The accounts contained information including participants' Social Security numbers and may have included other information such as names, HealthEquity member ID, account type (HSA, HRA, FSA, LPFSA, DCRA), contribution amount, and employer's name.

While we have no evidence that any personal information has been misused, we want to provide you with tools and resources to help protect your information.

What we are doing
Following the discovery, HealthEquity took several steps to address the incident including:

- Immediately securing the accessed email accounts
- Alerting law enforcement
- Completing a comprehensive third-party review of accessed accounts for personal information
- Verifying no other HealthEquity email accounts or systems were accessed
- Conducting a third-party audit of HealthEquity's systems to detect and prevent unauthorized logins

We are offering identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 5 years of credit monitoring, Cyberscan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. You will need to reference the enrollment code provided above when calling or enrolling on the website, so please do not discard this letter.

What you can do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 877.916.8380 or by going to https://ide.myidcare.com/healthequityprotect and using the enrollment code provided above. Please note the deadline to enroll is March 31, 2019. Also, please review the section of this notice titled "Important Information: Recommendations You Can Take to Protect Your Identity." It contains additional information about steps you can take to avoid identity theft.

For more information
HealthEquity has established a dedicated call center available at 877.916.8380 to answer questions and provide further information regarding this incident. You can find additional information and FAQs at https://ide.myidcare.com/healthequityprotect. The call center is open from 8 am – 8 pm Eastern. HealthEquity Member Services is also available 24/7 to assist you at 866.346.5800.

We sincerely apologize for this incident and are working hard to make it right.

Sincerely,

Jon Kessler
President and CEO
HealthEquity

Important Information: Recommendations You Can Take to Protect Your Identity

Review Your Accounts and Credit Reports

You should regularly review statements from your accounts and periodically obtain your credit report from one or more of the national consumer reporting agencies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. You may also contact one or more of the three national consumer reporting agencies listed below.

Fraud Alerts and Security Freezes

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the credit reporting agencies listed below.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You may now freeze and unfreeze your credit file for free, and do so online, by phone, or by mail.

You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To request a security freeze, you may need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	www.freeze.transunion.com
www.equifax.com	www.experian.com	www.transunion.com

Additional Steps to Avoid Identity Theft

- ***Be vigilant and review financial accounts and credit reports to detect suspicious activity.*** Notify your financial institutions of any unusual activity.
- ***Contact your local Social Security Administration office to notify them of any potential identity theft.*** Additional information regarding your Social Security Number can be found online at: www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.
- ***Be Suspicious of Phishing Emails.*** We will not at any time request that you submit personal information by e-mail. If you receive an email requesting personal information or log-in credentials that seems to come from us, do not respond to it, click on a link in the email, or open any attachments in the email. Please report such emails to privacy@healthequity.com.

Suggestions If You Are a Victim of Identity Theft

- ***File a police report*.** You should report instances of known or suspected identity theft to law enforcement, the Federal Trade Commission, and your state Attorney General. The FTC and your State Attorney General can also provide information about steps to avoid identity theft. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.
- ***Contact the U.S. Federal Trade Commission (FTC).*** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1- 877-IDTHEFT (438-4338); online at www.identitytheft.gov; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft," from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf. The FTC also has additional information about security freezes and fraud alerts.
- ***Keep a record of your contacts*.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

State Specific Information

For Maryland residents, in addition to the FTC and credit reporting agencies, you can obtain more information about steps to avoid ID theft from the Attorney General who can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; tel. 1-888-743-0023; and www.oag.state.md.us. **For New Mexico residents,** 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 www.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. **For North Carolina residents,** in addition to the FTC and credit reporting agencies, you can obtain more information about steps to avoid ID theft from the Attorney General who can be reached at: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov.