BRYAN CAVE LEIGHTON PAISNER LLP
161 North Clark Street, Suite 4300, Chicago, IL 60601-3315
T: 312 602 5000 F: 312 602 5050 bclplaw.com

June 13, 2018

Jena M. Valdetero
Direct: 312/602-5056
Fax: 312/698-7456
jena.valdetero@bclplaw.com

CONFIDENTIAL
VIA FEDEX

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Security Breach Notification

To Whom It May Concern:

In compliance with relevant state law, HealthEquity, Inc. ("HealthEquity"), a client of Bryan Cave Leighton Paisner LLP, is providing notice that HealthEquity is in the process of notifying individuals who reside in your state of an email account compromise that affected the personal information of certain employees who worked for companies that partner with HealthEquity. HealthEquity is a provider of healthcare accounts, including health savings accounts (HSAs) and reimbursement accounts such as flexible spending accounts, health reimbursement arrangements, limited purpose flexible spending accounts, and dependent care reimbursement accounts. Letters are being sent by first class U.S. mail to consumers starting on June 12, 2018, and HealthEquity anticipates final letters being transmitted no later than June 20, 2018.

HealthEquity is providing you this notice on behalf of itself and multiple employers and health plans that were impacted and have been notified. Please contact me if you would like more information concerning those entities.

As described in the sample notices attached to this letter, an unauthorized individual was able to gain access to one email account of a HealthEquity employee on April 11, 2018. The unauthorized individual used his access to send phishing emails from that account to numerous individuals on April 13, 2018. HealthEquity discovered the unauthorized access on April 13, 2018, and excluded the unauthorized individual from the email account. Although we have no evidence that the unauthorized third individual viewed or downloaded any of the emails in the team member's inbox, HealthEquity cannot conclusively rule out this possibility. An investigation by a third party forensics firm determined that this incident was limited to one email account for one HealthEquity employee, and did not affect any other HealthEquity systems.

A forensic review of the contents of the mailbox by the forensic investigator and outside legal counsel was completed on May 25, 2018, to identify documents that may have contained personally identifiable information (PII) or protected health information (PHI). The review identified a small number of emails and attachments that included certain personal information of HealthEquity's partners' employees.

As you will see in the attached notification letters, HealthEquity is providing different versions of its notification letter to individuals to match the personal information that may have been affected.

- Recipients of Letter Version A had health reimbursement arrangements (HRAs) or flexible spending accounts (FSAs) administered by HealthEquity and may have had their name, HealthEquity member ID, account type (*e.g.*, HRA or FSA), deduction amount, their employer's name and social security number exposed in this incident.
- Recipients of Letter Version B had health reimbursement arrangements or flexible spending accounts administered by HealthEquity and may have had their name, HealthEquity member ID, employer name, HealthEquity employer ID, claim type, deduction amount, patient name, service date, payee, date processed, HealthEquity claim ID, and healthcare account type exposed in this incident. At this time, we have no reason to believe that social security numbers were exposed for Letter Version B recipients.
- Recipients of Letter Version B1 had health reimbursement accounts administered by HealthEquity and may have had their name, HealthEquity member ID, employer name, HealthEquity employer ID, claim type, deduction amount, patient name, service date, payee, date processed, HealthEquity claim ID, and healthcare account type exposed in this incident. At this time, we have no reason to believe that social security numbers were exposed for Letter Version B1 recipients.
- Recipients of Letter Version C had health savings accounts administered by HealthEquity and may have had their HealthEquity member ID, first/middle name, last name, social security number, and employer name exposed in this incident.

The following chart shows the number of individuals in your state receiving each version of the letter:

Letter Version A Recipients	Letter Version B Recipients	Letter Version B1 Recipients	Letter Version C Recipients	Total
3	0	0	13	16

Law enforcement has been notified. HealthEquity is providing affected individuals whose social security numbers were contained in the documents identified in the mailbox with 5 years of ID Experts' credit monitoring and identity theft protection services. For individuals whose information was identified but was not associated with social security numbers, HealthEquity is providing 1 year of credit monitoring and identity theft protection services. Information regarding these services, as well as additional information to assist individuals, is

included in the notification sent to the affected individual. HealthEquity has set up a call center and website through ID Experts to address any questions or concerns from impacted individuals. HealthEquity has adopted enhanced security practices to prevent a similar incident from occurring in the future, including the implementation of additional technical security measures and retraining and reeducation of its workforce, and is actively monitoring accounts for any suspicious activity.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Jena Valdetero

Jena Valdetero

Attachment

ATTACHMENT

Letter Version A

HealthEquity
Building Health Savings

To Enroll, Please Call:
(888) 262-1560
Or Visit:
https://ide.myidcare.com/healthequity
Enrollment Code: [XXXXXXXX]

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

«Employee_First_Name» «Employee_Last_Name»
«Street_Address_1»
«Street_Address_2»
«City_State_Zip»

June 12, 2018

Dear «Employee_First_Name» «Employee_Last_Name»:

Re: ***Notice of Data Breach***

We are writing to inform you of a privacy incident related to information you provided when opening your health reimbursement arrangement (HRA) or flexible spending account (FSA). HealthEquity, Inc. ("HealthEquity") manages these accounts for your employer. This incident only affects the systems of HealthEquity, not those of your employer. This letter provides you with information concerning the incident as well as detailed information about steps we have taken to mitigate the effects of this incident.

What Happened
On April 11, 2018, an unauthorized individual gained access to one email account for a HealthEquity employee. The individual used his access to send phishing emails from that account to numerous individuals. HealthEquity discovered the unauthorized access on April 13, 2018, and excluded the individual from the email account. However, during the time that the individual had access to the account it is possible, but we cannot confirm, that the contents of the mailbox may have been downloaded. Unfortunately, the email account contained a spreadsheet attachment that included personal information about you.

We sincerely apologize for what happened, and we remain committed to protecting the security and confidentiality of your information.

What Information Was Involved
It is not clear whether your information was used for any inappropriate purposes. The spreadsheet contained your name, HealthEquity member ID, account type (e.g., HRA or FSA), deduction amount, and social security number. Your employer's name was contained in the email to which the spreadsheet was attached.

What We Are Doing
HealthEquity immediately launched an investigation and secured the employee's email account to prevent further exposure. HealthEquity is adopting new security practices to prevent a similar incident from occurring in the future, including the implementation of technical security measures and retraining and reeducation of its workforce. In addition, 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: 60 months of Credit Monitoring, Cyberscan Dark Web Monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials 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 following 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 (888) 262-1560 or going to https://ide.myidcare.com/healthequity and using the enrollment code provided above. MyIDCare experts are available Monday through Friday from 8am - 8pm Eastern Time. Please note the deadline to enroll is September 12, 2018.

For More Information

HealthEquity has established a dedicated call center through our vendor, ID Experts, available at (888) 262-1560 to answer questions and provide further information regarding this incident. Additional information about protecting your identity is enclosed.

Sincerely,

Trinity Car, Director of Privacy
HealthEquity, Inc.

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. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. 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 will 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, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 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,** the Attorney General can be contacted by mail 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.

Letter Version B

HealthEquity
Building Health Savings

15 West Scenic Pointe Drive, Suite 100
Draper, UT 84020

Date

«Employee_First_Name» «Employee_Last_Name»
«Street_Address_1»
«Street_Address_2»
«City_State_Zip»

Dear *Mr./Ms.* «Employee_Last_Name»:

Re: ***Notice of Data Breach***

We are writing to notify you of a privacy incident related to information you provided in connection with your health reimbursement arrangement (HRA) or flexible spending account (FSA), which HealthEquity administers. HealthEquity provides reimbursement arrangement services to team members of your employer, and your information was provided to us in connection with the services we provide. This incident only affects one email account of one HealthEquity employee, not any systems of your employer. This letter provides you with information concerning the incident as well as detailed information about steps we have taken to mitigate the effects of this incident.

What Happened
On April 11, 2018, an unauthorized individual gained access to one email account for a HealthEquity employee. HealthEquity discovered the unauthorized access on the morning of April 13, 2018, and blocked the unauthorized individual's access to the email account. However, during the time that the unauthorized individual had access to the email account it is possible, but we cannot confirm, that the contents of the mailbox may have been downloaded. A forensic analysis completed on May 25, 2018, identified some of your employees' personal information was contained in the email account. We sincerely apologize for what happened. We remain committed to protecting the security and confidentiality of your information.

What Information Was Involved
It is not clear whether your information was used for any inappropriate purposes. The information that may have been exposed may have included your name, HealthEquity member ID, employer name, HealthEquity employer ID, claim type, deduction amount, patient name, service date, payee, date processed, HealthEquity claim ID, and healthcare account type (e.g., FSA, HRA, or LPFSA). At this time, we have no reason to believe that social security numbers were exposed.

What We Are Doing
HealthEquity immediately launched an investigation and secured the employee's email account to prevent further exposure. HealthEquity has adopted new security practices to prevent a similar incident from occurring in the future, including the implementation of technical security measures and retraining and reeducation of its workforce. In addition, 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: 12 months of Credit Monitoring, Cyberscan Dark Web Monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials 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 when calling or enrolling on the website, so please do not discard this letter.

Your Enrollment Code: [ID Experts will insert]

What You Can Do
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (888) 262-1560 or going https://ide.myidcare.com/healthequity and using the enrollment code provided above. MyIDCare experts are available Monday through Friday from 8am - 8pm Eastern Time. Please note the deadline to enroll is September 12,

2018.

For More Information

HealthEquity has established a dedicated call center through our vendor, ID Experts, available at (888) 262-1560 to answer questions and provide further information regarding this incident. Additional information about protecting your identity is enclosed.

Sincerely,

Trinity Car, Director of Privacy
HealthEquity, Inc.

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. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. 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 will 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.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 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**, the Attorney General can be contacted by mail 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.

Letter Version B1

HealthEquity
Building Health Savings

15 West Scenic Pointe Drive, Suite 100
Draper, UT 84020

Date

«Employee_First_Name» «Employee_Last_Name»
«Street_Address_1»
«Street_Address_2»
«City_State_Zip»

Dear *Mr./Ms.* «Employee_Last_Name»:

Re: ***Notice of Data Breach***

We are writing to inform you of a privacy incident regarding information related to your health reimbursement account (HRA). HealthEquity is a subcontractor for Blue Cross and Blue Shield of NC (Blue Cross NC), which serves as the third party administrator for the State Health Plan. HealthEquity administered the HRA for members enrolled in the Consumer-Directed Health Plan (CDHP). The CDHP is no longer offered to Plan members, however, records are maintained by HealthEquity. This incident only affects one email account of one HealthEquity employee, not those of any other State Health Plan vendor. This letter provides you with information concerning the incident, as well as detailed information about steps we have taken to address this incident and its impact to you.

What Happened
On April 11, 2018, an unauthorized individual gained access to one email account for a HealthEquity employee. HealthEquity discovered the unauthorized access on the morning of April 13, 2018, and blocked the unauthorized individual's access to the email account. However, during the time that the unauthorized individual had access to the email account it is possible, but we cannot confirm, that the contents of the mailbox may have been downloaded. A forensic analysis completed on May 25, 2018, identified some of your employees' personal information was contained in the email account.

What Information Was Involved
It is not clear whether your information was used for any inappropriate purposes. The information that may have been accessed may include your name, HealthEquity member ID, employer name, HealthEquity employer ID, claim type, deduction amount, patient name, service date, payee, date processed, HealthEquity claim ID, and healthcare account type (e.g., FSA, HRA, or LPFSA). At this time, we have no reason to believe that Social Security numbers were exposed. We do not know whether your information has been used for any inappropriate purposes, or if it may be used for any inappropriate purposes in the future.

What We Are Doing
HealthEquity immediately launched an investigation and secured the employee's email account to prevent further exposure. HealthEquity has adopted new security practices to prevent a similar incident from occurring in the future, including the implementation of technical security measures and retraining and re-education of its workforce.

What We Are Offering
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: 12 months of Credit Monitoring, Cyberscan Dark Web Monitoring, a $1,000,000 insurance reimbursement policy, exclusive

educational materials 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 when calling or enrolling on the website, so please do not discard this letter.

Your Enrollment Code: [ID Experts will insert]

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (888) 262-1560 or going https://ide.myidcare.com/healthequity and using the enrollment code provided. MyIDCare experts are available Monday through Friday from 8am - 8pm Eastern Time. Please note the deadline to enroll is September 12, 2018.

For More Information

HealthEquity has established a dedicated call center through our vendor, ID Experts, available at (888) 262-1560 to answer questions and provide further information regarding this incident. Additional information about protecting your identity is enclosed.

We sincerely apologize for this incident. We remain committed to protecting the security and confidentiality of your information.

Sincerely,

Trinity Car, Director of Privacy
HealthEquity, Inc.

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 agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

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. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. 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 will 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
freeze.equifax.com	experian.com/freeze/	freeze.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.

For North Carolina residents, the Attorney General can be contacted by mail 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 Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 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 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.

Letter Version C

HealthEquity

To Enroll, Please Call:
(888) 262-1560
Or Visit:
https://ide.myidcare.com/healthequity
Enrollment Code: [XXXXXXXX]

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

«Employee_First_Name» «Employee_Last_Name»
«Street_Address_1»
«Street_Address_2»
«City_State_Zip»

June 14, 2018

Dear «Employee_First_Name» «Employee_Last_Name»:

Re: ***Notice of Data Breach***

We are writing to inform you of a privacy incident regarding information related to your health savings account (HSA) managed by HealthEquity, Inc. ("HealthEquity"). This letter provides you with information concerning the incident as well as detailed information about steps we have taken to address this incident and its impact to you.

What Happened
On April 11, 2018, an unauthorized individual gained access to one email account for a HealthEquity employee. HealthEquity discovered the unauthorized access on April 13, 2018, and blocked the unauthorized individual's access to the email account. However, during the time that the unauthorized individual had access to the account it is possible, but we cannot confirm, that the contents of the mailbox may have been downloaded. A comprehensive forensic analysis of the mailbox was completed on May 25, 2018, which identified that some of your personal information was contained in the email account. We sincerely apologize for what happened. We remain committed to protecting the security and confidentiality of your information.

What Information Was Involved
It is not clear whether your information was used for any inappropriate purposes. The personal information potentially exposed was: HealthEquity member ID, first/middle name, last name, social security number, and employer name.

What We Are Doing
HealthEquity immediately launched an investigation and secured the employee's email account to prevent further exposure. HealthEquity has adopted new security practices to prevent a similar incident from occurring in the future, including the implementation of technical security measures and retraining and reeducation of its workforce. In addition, 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, exclusive educational materials 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 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 (888) 262-1560 or going https://ide.myidcare.com/healthequity and using the enrollment code provided above. MyIDCare experts are available Monday through Friday from 8am - 8pm Eastern Time. *Please note the deadline to enroll is September 12, 2018.*

For More Information

HealthEquity has established a dedicated call center through our vendor, ID Experts, available at (888) 262-1560 to answer questions and provide further information regarding this incident. Additional information about protecting your identity is enclosed.

Sincerely,

Trinity Car, Director of Privacy
HealthEquity, Inc.

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. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. 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 will 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.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 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**, the Attorney General can be contacted by mail 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.