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

November 15, 2018

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

**CONFIDENTIAL**
**VIA EMAIL**

Washington Attorney General
securitybreach@atg.wa.gov

Re: Data Security Breach Notification

To Whom It May Concern:

Pursuant to relevant state law, HealthEquity, Inc. ("HealthEquity"), a client of Bryan Cave Leighton Paisner LLP (our "Firm"), is providing notice of a data security breach to your office. HealthEquity has notified or will soon notify individuals who reside in your state that two corporate email accounts were compromised that potentially exposed personal information. HealthEquity, either directly or in association with employers and health plans, provides services designed to give individuals tax advantages to offset health care costs, including health savings accounts ("HSAs"), health reimbursement arrangements ("HRAs"), health flexible spending arrangements ("FSAs"), limited purpose FSAs ("LPFSAs"), and dependent care reimbursement accounts ("DCRAs"). HSAs are individual custodial accounts, and HRAs, FSAs, LPFSAs, and DCRAs are employer plans (see, e.g., IRS Publication 969). The incident also involved HealthEquity employee health plan enrollment information.

Letters to affected individuals were sent by first class U.S. mail to consumers starting on November 15, 2018, and final letters will be transmitted no later than November 27, 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, on October 5, HealthEquity's information security team identified unauthorized logins to two HealthEquity employees' email accounts. The team immediately implemented security measures to prevent further access to the email 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. Although we have no evidence that the unauthorized individual viewed any of the emails in the email accounts, HealthEquity cannot conclusively rule out this possibility. An investigation by a third-party forensics firm determined that this incident was limited to two email accounts and did not affect any other HealthEquity systems.

Our Firm began providing the initial results of a forensic review of the contents of the mailbox on October 20, 2018, to identify documents that may have contained personally identifiable information

("PII"). The review identified a number of emails and attachments that included certain PII. HealthEquity began notifying its health plans and business partners on October 22, 2018.

As indicated in the attached notification letter samples, HealthEquity is providing different versions of its notification letter to individuals to match the PII that may have been exposed. Example draft versions of these letters are attached to this notice.

- Recipients of Version A had an account administered by HealthEquity and may have had their name and Social Security number exposed.
- Recipients of Version B had an account administrated by HealthEquity and may have had their name, Social Security number, account type (HSA, HRA, FSA, LPFSA, DCRA), and employer's name exposed. This version was drafted in conjunction with a health plan partner.
- Recipients of Version C had an account administered by HealthEquity and may have had their name, Social Security number, account type (HSA, HRA, FSA, LPFSA, DCRA), and associated employer or plan exposed. This version was drafted in conjunction with a health plan partner.
- Recipients of Version D are employees or former employees (and their dependents) of HealthEquity whose health plan enrollment data may have been exposed.

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

| Version A | Version B | Version C | Version D | Total |
|---|---|---|---|---|
| 2,030 | 24,027 | 1,112 | 6 | 27,175 |

In addition, law enforcement has been notified. The U.S. Department of Health and Human Services Office for Civil Rights will be notified on November 16, 2018.

HealthEquity is providing affected individuals with 5 years of ID Experts' 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 individuals. 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 incident, please contact me at your convenience.

Sincerely,

/s/ Jena Valdetero

Jena Valdetero

Attachment

**ATTACHMENT**

# 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.

# Version B

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 19, 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 related to certain participants in HealthEquity plans. HealthEquity provides health savings account (HSA), flexible spending account (FSA) and health reimbursement arrangement (HRA) administration for your employer. 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 contained other information such as names, HealthEquity member ID, account type (HSA, HRA, FSA, LPFSA, DCRA), deduction 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 going 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**

## HealthEquity's Nondiscrimination Notice and Access to Communication Services

HealthEquity, Inc.'s ("HealthEquity") primary purpose is to provide non-health services to holders of health savings accounts. In addition to these services, HealthEquity provides services to, and on behalf of, health plans. HealthEquity and the health plans do not exclude people or treat them unfairly because of sex, age, race, color, national origin or disability.

Free services are available to help you communicate with us and with your health plan, including providing letters in other languages or in other formats, such as large print. If you need help, please call the toll-free number on your benefits card. For language assistance on your call, simply ask for an interpreter.

If you think you were not treated fairly because of your sex, age, race, color, national origin, or disability, you can send a complaint to:

HealthEquity, Inc.
Attention: Director of regulatory services
15 W. Scenic Pointe Dr.
Draper, UT 84020
Fax: (801) 206-3895
Email: RegulatoryServices@HealthEquity.com

Upon receiving your complaint, we will work with your health plan to address your concerns. If you need help with your complaint, please call the toll-free number on your member ID card. You must send the complaint within 60 days of when you found out about the issue.

You can also file a complaint with the United States Department of Health and Human Services
online https://ocrportal.hhs.gov/ocr/portal/lobby.jsf
Complaint forms are available at http://www.hhs.gov/ocr/office/file/index.html.
Phone: Toll-free 1-800-368-1019, 800-537-7697 (TDD)
Mail: U.S. Dept. of Health and Human Services. 200 Independence Avenue, SW Room 509F, HHH Building
Washington, D.C. 20201

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 866.346.5800.
注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 866.346.5800.

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 866.346.5800.

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 866.346.5800.

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 866.346.5800.
주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 866.346.5800

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 0085.643.668

注意事項：日本語を話される場合、無料の言語支援をご利用いただけます。866.346.5800.

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 866.346.5800.

ATTENTION : Si vous parlez français, des services d’aide linguistique vous sont proposés gratuitement. Appelez le 866.346.5800.

เรยี น: ถ้าคณุพูดภาษาไทยคณุสามารถใช้บรกิารช่วยเหลือ ทางภาษาไดฟร ี โทร 866.346.5800.

**ت وجه:** اگر ب ه زبان فارسی گفتگو می کنید، ب ا شما ف راهم می ب اشد. ب رای تس هیلات زب انی ب صورت رای گان ب ا 866.346.5800 تماس بگیری د.

УВАГА! Якщо ви розмовляєте українською мовою, ви можете звернутися до безкоштовної служби мовної підтримки. Телефонуйте за номером 866.346.5800.

ATENȚIE: Dacă vorbiți limba română, vă stau la dispoziție servicii de asistență lingvistică, gratuit. Sunați la 866.346.5800.

## 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.

# Version C

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 XX, 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. HealthEquity is one of the nation's largest providers of health savings accounts (HSAs) and reimbursement arrangement services (flexible spending accounts, health reimbursement accounts, limited purpose flex spending accounts, and dependent care reimbursement accounts, etc.). HealthEquity provides reimbursement arrangement services to employers and health plans, and your information was provided to HealthEquity in connection with the services we provide.

**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 affected, and initiated an investigation to determine the nature of the incident.

On October 22, 2018, HealthEquity notified your health plan or associated employer that it was investigating this incident and its potential impact to participants' sensitive personal information. Through the investigation we determined that your information was located in an impacted email account accessed on October 5, 2018.

**What information was involved**
The email account contained documents that included personal information that HealthEquity uses to manage member accounts for legitimate business purposes. The following information about you was contained in one of the email accounts impacted: first name, last name, social security number and employer/group name.

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

- Immediately preventing further unauthorized access to the email account affected
- Alerting law enforcement
- Engaging a nationally recognized third party forensic firm to complete an independent and comprehensive investigation into the incident
- Completing a comprehensive third-party review of accessed accounts for personal information
- Verifying no other HealthEquity email accounts or systems were affected
- Conducting a third-party audit of HealthEquity's systems to strengthen security controls and protocols and evaluating training and policies and procedures designed to prevent future occurrence

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 discard this letter."

**What you can do**
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.

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.

# Version D

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 XX, 2018

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

NOTICE OF DATA BREACH

We are writing to provide information about a recent data security incident at HealthEquity. 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 team members and, in some cases, their dependents. 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 HealthEquity employee and, in some cases, dependent health plan enrollment information including Social Security numbers, names, insurance member ID, date of birth, and other sensitive personal information.

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 ard 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.