

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a recent data security incident (“Incident”) affecting a dedicated email inbox that US HealthCenter (“USHC”) uses to administer the Wellness Program of our client, Cost Plus World Market (“Cost Plus”) that may have resulted in the disclosure of some of your protected health information (“PHI”). We take the privacy and protection of your personal information very seriously. Your trust is a top priority, and we deeply regret any inconvenience this may cause. At this time, we have no evidence that your information has been misused. Out of an abundance of caution, this letter contains information about what happened, and steps we have taken to mitigate the risk.

As you may know, USHC has administered the Cost Plus wellness program for its employees for many years. Among other things, USHC hosts a dedicated email inbox utilized by Cost Plus wellness program participants to submit completed Annual Preventive Screening affidavits and to ask program questions. The purpose of this letter is to notify you that USHC has determined there was unauthorized access to this inbox.

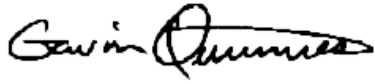
On April 13, 2020, we were made aware of unauthorized access to USHC’s dedicated Cost Plus email account. This account was used to distribute phishing emails to Cost Plus wellness plan participants in an attempt to gain access to participant personal information. USHC’s internal information security (IT) team conducted an investigation of the compromised account. USHC discovered that there was unauthorized access to the email account, and the individual(s) responsible were able to view and forward emails associated with this inbox. USHC then proceeded to conduct a comprehensive manual review of the contents of the email account to determine the specific type of data that may have been accessible by an unauthorized party. USHC’s investigation revealed that the compromised account contained forms submitted by Cost Plus plan participants, including an Annual Preventive Screening affidavit which may have contained a participant’s name, employee number, date of birth, physician signature, and date of exam. Apart from additional limited health information that you may have included in your email, the inbox in question did not contain participants’ social security numbers, drivers’ license numbers, credit card data, financial account information, insurance information, or other sensitive personal information. Based on its manual review of the contents of the email account, USHC worked with Cost Plus to identify the affected population along with their contact information for notification purposes. This process was completed in June 2020. Once the affected population was identified, USHC worked with Cost Plus to draft the appropriate notification letters to individuals and regulators.

Upon discovery of the unauthorized access to the inbox, USHC immediately changed all passwords associated with the inbox. In addition, the Cost Plus wellness program inbox is now being hosted on a new Microsoft Office 365 email platform with heightened security features, and USHC is enabling two-factor authentication for all email accounts.

Please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (“FTC”) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspect activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

Please know that safeguarding your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause to you and to Cost Plus. If you have any questions, please do not hesitate to contact our dedicated call center at telephone number [1-800-833-3333](tel:1-800-833-3333), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink that reads "Gavin Quinnies". The signature is written in a cursive style with a long, sweeping underline.

Gavin Quinnies
President & CEO
US HealthCenter, Inc.

Additional Important Information

For residents of **Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina**: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001
1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.