



Health Net®

21650 OXNARD STREET
WOODLAND HILLS, CA 91367
818-676-8017
818-676-5933 (FAX)

Identity Theft

FACSIMILE TRANSMITTAL SHEET

TO: The Honorable Tom Miller

FROM: Patricia T. Clarey, SVP, Chief
Regulatory & External Relations Officer

COMPANY:

Iowa Attorney General

DATE:

March 14, 2011

FAX NUMBER:

515-281-4209

NUMBER OF PAGES INCLUDING COVER:

8/10

PHONE NUMBER:

RE: Security Incident

NOTES/COMMENTS:

The documents accompanying this facsimile transmission may contain confidential information. The information is intended only for the use of the individual or entity named above. If you are not the intended recipient, or the person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the information contained in this transmission is strictly PROHIBITED. If you have received this transmission in error, please notify the sender immediately by telephone or by return FAX and destroy this transmission, along with any attachments. Thank you.



Health Net, Inc.
21650 Oxnard Street
Woodland Hills, CA 91367

March 14, 2011

The Honorable Tom Miller
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
Fax: (515) 281-4209

Dear Mr. Attorney General:

We write to inform you about a recent information security incident involving the personal information of certain former and current Health Net members, employees, and health care providers.

On January 21, 2011, IBM, Health Net's vendor responsible for managing Health Net's IT infrastructure, notified Health Net of an inventory discrepancy regarding certain server drives. Specifically, IBM informed us that the company could not locate several hard disk drives that were being decommissioned as part of the move of Health Net's data center operations from Rancho Cordova, California to IBM's facility in Boulder, Colorado. We promptly began an investigation of the incident, which is continuing. The incident also was reported to local authorities in Rancho Cordova, California. Based on our investigation, we have reason to believe that the hard disk drives contained Health Net members', employees' and health care providers' personal information, which may include names, addresses, health information, Social Security numbers and/or financial information. We are continuing to take steps (including working with external security specialists) to investigate this incident, further enhance our security and help prevent this type of incident from happening in the future.

Approximately 2,333 individuals who may be affected by this incident are residents of your state or jurisdiction. While the investigation continues, Health Net has made the decision out of an abundance of caution to notify affected individuals. Attached for your reference are copies of the notices that Health Net will send to the affected individuals. We will mail the notices to the affected individuals starting the week of March 14, 2011.

As more fully described in the attached notices, Health Net will offer the affected individuals two years of free identity protection through the Debix Identity Protection Network. These services also include \$1 million in identity theft insurance coverage and reimbursement for any fees associated with applying or thawing a credit freeze.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Patricia T. Clarey
SVP, Chief Regulatory & External Relations Officer
Health Net, Inc.
21650 Oxnard Street
Woodland Hills, California 91367
818-676-5394
patricia.t.clarey@healthnet.com



Processing Center, P.O. Box 3825, Suwanee, GA 30024

**Free Identity Protection**

Activation Code: 155492036

Enroll at www.debix.com/healthnet

Assistance Hotline: (855) 434-8081

99 99 9999 *****AUTO**SCH 3-DIGIT 917
John Q Sample
123 Anystreet
Anytown, US 12345-6789



March 14, 2011

Dear John Q Sample,

We are writing to inform you of an incident involving the personal information of certain former and current Health Net members.

On January 21, 2011, IBM, which handles Health Net's data center operations, notified Health Net of an information security incident. Specifically, IBM informed us that the company could not locate several hard disk drives that had been used in Health Net's corporate servers and that IBM was handling on behalf of Health Net. We promptly began an investigation of the incident, which is continuing. Based on our investigation, we have reason to believe that information that pertains to you is included on the hard disk drives. The information included details such as your name, address, and health information. ***Neither your Social Security number nor financial information was included in the information on the drives.*** We are writing to tell you about the incident out of an abundance of caution and to call your attention to the steps you may take to help protect yourself.

To help safeguard you from misuse of your personal information, we have arranged for you to receive two years of identity protection through the Debix Identity Protection Network, at no cost to you. If the recipient of this letter is under the age of eighteen, we have arranged for the individual to receive two years of identity theft protection services with Debix ChildScan. To receive this identity protection service, you must register within 120 days from the date of this letter using the activation code listed at the top of this letter. You may register for the identity protection service online at www.debix.com/healthnet, by mail using the enclosed mail-in registration form, or by calling (855) 434-8081. We have enclosed a Reference Guide that describes the Debix Identity Protection Network services in detail, explains the registration process, and suggests other steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file. Additionally, Health Net has arranged for you to be reimbursed for any fees associated with applying or thawing a credit freeze for a two year period. To learn more, please contact Debix at (855) 434-8081.

Whether or not you choose to enroll in the free Debix Identity Protection Network service, you should continue to check your credit report periodically to ensure fraudulent activity has not occurred. Even if you do not find any signs of fraud on your report, we recommend that you remain vigilant and check your credit report periodically. We also recommend that you regularly review the explanation of benefit statements you receive from Health Net. If you see any service that you believe you did not receive, please contact Health Net at the phone number specified on your statement.

Keeping your personal information secure is of the utmost importance to us. We sincerely regret any inconvenience or concern this event may cause you. In the meantime, we urge you to take advantage of the



services available to you. We are taking steps to enhance our security and to help prevent this type of incident from happening in the future.

If you have questions regarding this incident or the Debix Identity Protection Network, please call (855) 434-8081 toll-free Monday through Saturday, 7:00 a.m. to 7:00 p.m. PST (TTY/TDD use 711).

Sincerely,



James Woys
Chief Operating Officer
Health Net, Inc.

Reference Guide

In addition to other details, this Reference Guide includes information suggested by the following states: Hawaii, Iowa, Maryland, Massachusetts, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming.

We encourage individuals receiving this letter to take the following steps:

Register for Credit Monitoring. To receive two years of identity protection under the Debix Identity Protection Network, please register 120 days from the date of this letter, as explained in the "How to Enroll" section below. Debix has indicated that its service includes:

- **OnCall Credit Alerts** – you will receive actionable OnCall Credit Alerts by phone when there are changes in your credit file.
- **OnCall Investigation Team** – live OnCall investigators will assist you if an issue occurs related to this incident, and will help file cases with law enforcement.
- **OnCall Attack Reports** – this allows Health Net to know if data is being used by identity thieves.
- **\$1 Million Insurance** – this service includes comprehensive identity restoration and \$1 million in identity theft insurance coverage to correct fraud.
- **Debix Recovery Services** – this service provides assistance in restoring your credit file.

From the date that you establish your account, Debix will enroll you in OnCall Credit Monitoring and you will receive OnCall Credit Alerts regarding changes in your credit file. Using your phone, you can review and verify these credit alerts. Debix OnCall investigators are available to assist you in the event that you suspect fraud.

How to Enroll. You will need to provide the activation code that is listed below. You may register online at www.debix.com/healthnet, by mail using the enclosed mail-in registration form, or by phone by calling (855) 434-8081 toll-free Monday through Saturday, 7 a.m. to 7 p.m. PST (TTY/TDD use 711). Activation codes are specific to each individual and cannot be used multiple times.



Free Identity Protection

Activation Code: 155492036
Enroll at www.debix.com/healthnet
Assistance Hotline: (855) 434-8081

Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus.

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

When you receive your credit report, review it carefully. Look for accounts you did not open (note that some companies bill under names other than their store names; the credit bureau will be able to tell you when that is the case). Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Look in the "personal information" section for any inaccuracies in your information, such as home address and Social Security number. If you see anything you do not understand, call the credit bureau at the telephone number specified in the report. Errors in this information may be a warning sign of possible identity theft.

You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. If you find items you do not understand on your report, call the credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Federal Trade Commission (FTC) Recommendations. If you detect any unauthorized transactions in your financial account, promptly notify your financial institution or your debit or credit card company. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

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

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

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

Equifax
P.O. Box 740241
Atlanta, Georgia 30374-0241
877-478-7625
www.equifax.com

Experian
P.O. Box 9532
Allen, Texas 75013
888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
800-680-7289
www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit report at the three national credit bureaus without your consent. There may be fees for placing, lifting or removing a security freeze, which generally range from \$5 to \$20 per action. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau.* Because the instructions for how to establish a security freeze differ from state to state, please contact the three credit bureaus to find out more information.

Equifax
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, Texas 75013
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
www.transunion.com

The credit bureaus may require you to verify your identity prior to placing a security freeze on your credit file. You may be asked to provide information such as your full name with middle initial and generation; your Social Security number; your date of birth; proof of your current residential address; addresses where you have lived over the past five years; and a legible copy of a government-issued ID.

For Maryland Residents. You may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General. You can contact the Maryland Office of the Attorney General at:

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

For Massachusetts Residents. The credit bureaus may charge you a fee of up to \$5 to place a freeze on your credit file, and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 919-716-6400 or 877-566-7226 (toll-free in North Carolina)
www.ncdoj.gov



Processing Center, P.O. Box 3825, Suwanee, GA 30024



Free Identity Protection

Activation Code: 159446038

Enroll at www.debix.com/healthnet

Assistance Hotline: (855) 434-8081

999 999 9999 *****AUTO**SCH 3-DIGIT 917

John Q Sample

123 Anystreet

Anytown, US 12345-6789



March 14, 2011

Dear John Q Sample,

We are writing to inform you of an incident involving the personal information of certain former and current Health Net members.

On January 21, 2011, IBM, which handles Health Net's data center operations, notified Health Net of an information security incident. Specifically, IBM informed us that the company could not locate several hard disk drives that had been used in Health Net's corporate servers and that IBM was handling on behalf of Health Net. We promptly began an investigation of the incident, which is continuing. Based on our investigation, we have reason to believe that information that pertains to you is included on the hard disk drives. The information included details such as your name, address, health information, Social Security number and your financial information. We are writing to tell you about the incident out of an abundance of caution and to call your attention to the steps you may take to help protect yourself.

To help safeguard you from misuse of your personal information, we have arranged for you to receive two years of identity protection through the Debix Identity Protection Network, at no cost to you. If the recipient of this letter is under the age of eighteen, we have arranged for the individual to receive two years of identity theft protection services with Debix ChildScan. To receive this identity protection service, you must register within 120 days from the date of this letter using the activation code listed at the top of this letter. You may register for the identity protection service online at www.debix.com/healthnet, by mail using the enclosed mail-in registration form, or by calling (855) 434-8081. We have enclosed a Reference Guide that describes the Debix Identity Protection Network services in detail, explains the registration process, and suggests other steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file. Additionally, Health Net has arranged for you to be reimbursed for any fees associated with applying or thawing a credit freeze for a two year period. To learn more, please contact Debix at (855) 434-8081.

Whether or not you choose to enroll in the free Debix Identity Protection Network service, you should continue to check your credit report periodically to ensure fraudulent activity has not occurred. Even if you do not find any signs of fraud on your report, we recommend that you remain vigilant and check your credit report periodically. We also recommend that you regularly review the explanation of benefit statements you receive from Health Net. If you see any service that you believe you did not receive, please contact Health Net at the phone number specified on your statement.

Keeping your personal information secure is of the utmost importance to us. We sincerely regret any



inconvenience or concern this event may cause you. In the meantime, we urge you to take advantage of the services available to you. We are taking steps to enhance our security and to help prevent this type of incident from happening in the future.

If you have questions regarding this incident or the Debix Identity Protection Network, please call (855) 434-8081 toll-free Monday through Saturday, 7:00 a.m. to 7:00 p.m. PST (TTY/TDD use 711).

Sincerely,



James Woys
Chief Operating Officer
Health Net, Inc.

Reference Guide

In addition to other details, this Reference Guide includes information suggested by the following states: Hawaii, Iowa, Maryland, Massachusetts, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming.

We encourage individuals receiving this letter to take the following steps:

Register for Credit Monitoring. To receive two years of identity protection under the Debix Identity Protection Network, please register 120 days from the date of this letter, as explained in the "How to Enroll" section below. Debix has indicated that its service includes:

- **OnCall Credit Alerts** – you will receive actionable OnCall Credit Alerts by phone when there are changes in your credit file.
- **OnCall Investigation Team** – live OnCall investigators will assist you if an issue occurs related to this incident, and will help file cases with law enforcement.
- **OnCall Attack Reports** – this allows Health Net to know if data is being used by identity thieves.
- **\$1 Million Insurance** – this service includes comprehensive identity restoration and \$1 million in identity theft insurance coverage to correct fraud.
- **Debix Recovery Services** – this service provides assistance in restoring your credit file.

From the date that you establish your account, Debix will enroll you in OnCall Credit Monitoring and you will receive OnCall Credit Alerts regarding changes in your credit file. Using your phone, you can review and verify these credit alerts. Debix OnCall investigators are available to assist you in the event that you suspect fraud.

How to Enroll. You will need to provide the activation code that is listed below. You may register online at www.debix.com/healthnet, by mail using the enclosed mail-in registration form, or by phone by calling (855) 434-8081 toll-free Monday through Saturday, 7 a.m. to 7 p.m. PST (TTY/TDD use 711). Activation codes are specific to each individual and cannot be used multiple times.



Free Identity Protection

Activation Code: 159446038
Enroll at www.debix.com/healthnet
Assistance Hotline: (855) 434-8081



Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus.

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

When you receive your credit report, review it carefully. Look for accounts you did not open (note that some companies bill under names other than their store names; the credit bureau will be able to tell you when that is the case). Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Look in the "personal information" section for any inaccuracies in your information, such as home address and Social Security number. If you see anything you do not understand, call the credit bureau at the telephone number specified in the report. Errors in this information may be a warning sign of possible identity theft.

You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. If you find items you do not understand on your report, call the credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Federal Trade Commission (FTC) Recommendations. If you detect any unauthorized transactions in your financial account, promptly notify your financial institution or your debit or credit card company. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

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

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

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



Equifax
P.O. Box 740241
Atlanta, Georgia 30374-0241
877-478-7625
www.equifax.com

Experian
P.O. Box 9532
Allen, Texas 75013
888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
800-680-7289
www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit report at the three national credit bureaus without your consent. There may be fees for placing, lifting or removing a security freeze, which generally range from \$5 to \$20 per action. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau.* Because the instructions for how to establish a security freeze differ from state to state, please contact the three credit bureaus to find out more information.

Equifax
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, Texas 75013
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
www.transunion.com

The credit bureaus may require you to verify your identity prior to placing a security freeze on your credit file. You may be asked to provide information such as your full name with middle initial and generation; your Social Security number; your date of birth; proof of your current residential address; addresses where you have lived over the past five years; and a legible copy of a government-issued ID.

For Maryland Residents. You may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General. You can contact the Maryland Office of the Attorney General at:

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

For Massachusetts Residents. The credit bureaus may charge you a fee of up to \$5 to place a freeze on your credit file, and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 919-716-6400 or 877-566-7226 (toll-free in North Carolina)
www.ncdoj.gov