

**Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
And Notification Act (General Business Law §889-aa;
State Technology Law §208)**

Name of Business, Individual or State Entity: Aetna Inc.

Date of Discovery of Breach: October 26, 2006

Estimated Number of Affected Individuals: 8,908 New York residents

Date of Notification of Affected Individuals: Notification will begin on Tuesday, December 5, 2006 and will be substantially complete by Friday, December 8, 2006

Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

On October 26, 2006 a theft occurred at an office complex where an Aetna subcontractor, Concentra Preferred Systems (Concentra), maintains a branch office. The theft *may* have resulted in the loss of approximately 130,758 health plan member records containing personal information, including Social Security Numbers. Based on our analysis, we estimate that approximately 8,908 New York residents were among the individuals whose information *may* have been disclosed as a result of this incident. The theft did not occur in the state of New York.

In its initial notification of the theft, Concentra reported that an Aetna laptop personal computer (PC) on loan to Concentra was one of the items stolen from its office. Because the laptop was encrypted using Pointsec encryption software and because the subcontractor did not store any personal information on the device, we concluded that no data breach had occurred and no action was necessary.

One week later, on November 3, Concentra informed Aetna that 36 computer server back-up tapes containing individual data had also been stolen in the same burglary. In addition to Concentra, five other tenants in the office complex were burglarized. The thieves took easily transportable items, including pharmaceuticals, cash, DVDs, and movie tickets, in addition to the Concentra tapes.

Although the information on the tapes was not encrypted, Concentra believes it to be very unlikely that data from the tapes could be accessed because of the complex combination of commercial equipment plus special versions of back-up and database software packages that would be necessary in order to read the data, which is itself in unlabeled formats that make it difficult to decipher.

Concentra consulted a third-party data analysis expert to determine the likelihood that the data could be successfully retrieved from the tape. The expert independently agreed that the likelihood was low.

In addition, law enforcement authorities believe that, based on the nature of the crime and the items taken from Concentra and other tenants in the building, this was the act of common thieves looking for cash and other property to convert to cash. There is no indication that personal data was specifically targeted.

As soon as we were aware that personal information was stored on the back-up tapes, we requested a copy of the data to determine which specific individuals had been impacted. Concentra provided us a readable file on Friday, November 10, but we still could not determine which individuals were impacted at that point because the vendor's file included only claim ID numbers for most records. None included addresses. Consequently, we had to perform extensive analysis to identify the specific individuals whose information was contained on the tapes and then develop accurate contact information for them by matching the information on the tapes with more complete medical claim and eligibility information in our company files.

Even though it is unlikely that the data on these tapes has been or will be retrieved by unauthorized persons, we nevertheless decided to err on the side of caution and notify the potentially affected individuals. Notification will begin on Tuesday, December 5, 2006. The notices urge the potentially affected individuals to place fraud alerts on their credit files and the notices also provide contact information for the following reporting agencies: Equifax, Experian and TransUnion.

Aetna will directly notify the three major consumer credit reporting agencies of this incident.

Name of Business Contact: Thomas A. Young
Title: Vice President and Chief Privacy and Security Officer
Telephone Number: (860) 273-7461

Email: YoungTA@Aetna.com

Date: December 4, 2006

Submitted by: Thomas J. Buchberger

Title: Senior Compliance Officer

Address: 151 Farmington Avenue, RE4K; Hartford, CT 06516

Email: BuchbergerTJ@Aetna.com

Telephone: (860) 273-4205

Dear (Member):

We want to inform you of a recent incident that may affect some Aetna plan members and former plan members, including you.

A burglary occurred at a field office of a company that provides medical claim audit services for many health plans including Aetna. Several other business tenants in the same office building were broken into, as well. Random items were stolen from each business, ranging from cash to DVD players, including a lockbox that contained our vendor's computer back-up cassette tapes. Some of the back-up tapes contained Aetna claim data, including personal member information.

At this time, we have no reason to believe this incident will lead to fraudulent credit applications or other identity theft crimes. The authorities believe that, based on the nature of the crime, the thieves were seeking property that could be easily sold for cash and that identity theft was not their intended goal.

The information contained on the data tapes would be difficult to access. It would require an unusual type of tape drive not found on common computers, plus a complex combination of commercial backup and database software that the vendor employed to create the back-up tapes.

Nevertheless, because some information about you was stored on the backup tapes that were taken, including your name, Social Security number (SSN) and hospital codes (indicating an area of the hospital that provided a service to you), we wanted to notify you about the incident. The tapes did not contain any personal banking information. Even though the risk of identity theft in this situation is small, we are offering you a credit monitoring service to identify any potential misuse of your personal information. The service is available at no cost to you.

Steps to Take to Protect Your Identity

We urge you to **place an initial fraud alert on your credit file**. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may call any one of the three major credit reporting companies. As soon as one credit reporting company confirms your fraud alert, the other credit agencies are notified to place a similar alert. An initial fraud alert stays on your credit report for 90 days and is available without charge.

Here is how you can contact the major credit reporting companies. Again, you only need to contact one, and the others will be notified:

- Equifax: 1-877-478-7625; www.equifax.com; P.O. Box 740241, Atlanta, GA, 30374-0241
- Experian: 1-888-397-3742; www.experian.com, P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Under federal law, you are entitled to a free copy of your credit report, at your request, from each of the major nationwide credit reporting companies once every 12 months. To order your free annual credit report from one or all of the national credit reporting companies, visit www.annualcreditreport.com, call toll free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from www.ftc.gov/credit.

Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name and employer(s). Notify the credit reporting companies if any information is incorrect.

Additional Credit Monitoring Assistance

In addition, we have arranged for you to enroll in a **3-in-1 monitoring service** through Equifax for a period of one year at no cost to you. Equifax 3-in-1 monitoring:

- Alerts you (daily via e-mail and wireless devices, and monthly via mail) to changes in credit card balances;
- Provides access to your Equifax Credit Report;
- Includes one Equifax, Experian and TransUnion 3-in-1 Credit Report;
- Provides access to live customer support upon enrollment; and
- Provides up to \$20,000 Identity Fraud Expense Coverage with no deductible (certain limitations and exclusions apply) † at no additional charge to you.

You will be able to enroll in the 3-in-1 monitoring service by using the Promotion Code listed in Step 3 below. In order to proceed with your registration and enroll for Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection service, you should contact Equifax via the Internet, as described below.

To take advantage of this offer, you must contact Equifax by March 15, 2007.

Internet Enrollment

Equifax has a simple Internet-based verification and enrollment process.

Visit: www.invservices.equifax.com/rti

Step 1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.

Step 2. Identity Verification: complete the form with your Social Security number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.

Step 3. Payment Information: During the "check out" process, provide the following Promotion Code: <XXXXXX> in the "Enter Promotion Code" box. (case sensitive, no spaces, include dash.) After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)

Step 4. Order Confirmation: – Click "View My Product" to access the product features and your credit reports.

If you do not have access to the Internet or wish for any other reason to enroll in Credit Watch by Mail with 3-in-1 Monitoring instead of the online service, please fill out the attached form and fax or mail it to the number/address listed on the form. You will also need the Promotion Code to enroll.

Individuals can find further general information about identity theft by accessing the:

- U.S. Federal Trade Commission site at
http://www.consumer.gov/idtheft/con_pubs.htm
- Federal Trade Commission site at
http://www.consumer.gov/idtheft/con_steps.htm

Every Aetna employee recognizes that members entrust us with their personal information. We have a comprehensive security program to protect that information. In addition, our vendors operate under contractual terms that require them to have safeguards in place to protect the privacy and security of member information. Unfortunately, in this circumstance, criminals burglarized a multi-tenant office building. Our vendor is assessing what additional security measures and action steps it could take to help prevent future occurrences. We are reviewing this vendor's overall security measures to confirm that safeguards are in place to help prevent similar incidents in the future.

Please contact us at 1-888-888-5724 if you have questions about this letter. This number has been established specifically to respond to your questions about this data security incident. Customer Service Representatives are available to respond to your questions Monday-Friday 8:00 A.M. to 9:00 P.M. Eastern Standard Time.

Thank you for your patience and understanding. We apologize for any inconvenience or concern this situation may cause you.

Sincerely,

Thomas A. Young
Vice President
Chief Privacy and Security Officer

† Identity Fraud Expense Reimbursement Master Policy underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on Equifax underwriting qualifications and state regulations. Coverage not available for residents of New York.
