

North Carolina Security Breach Reporting Form Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: Fiserv Health Plan Administrators, Inc. PLEASE SUBMIT FORM TO:
 Address: 1300 River Drive, Ste. 300, IL 008-1000 Consumer Protection Division
Moline, IL 61265-1368 NC Attorney General's Office
 Telephone: 309-736-4551 9001 Mail Service Center
 Raleigh, NC 27699-9001
 Fax: 800-484-8102 Telephone: (919) 716-6000
 Email: douglas - niska @ uhc . com Toll Free in NC: (877) 566-7226
 FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: 10/31/2008
 Date the Security Breach was discovered: 9/25/2008
 Estimated number of affected individuals: 125,000
 Estimated number of NC residents affected: 1,082

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): _____

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Laptop (encrypted) and external drive (not encrypted) stolen 9/25/2008, in San Antonio, TX

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. _____ If so, please describe the security measures protecting the information: See Above

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Employee violated existing policies and was terminated.

Date affected NC residents were/will be notified: Began this week

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (e): Recreation of data and other forensics to determine who may have been impacted.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))
 written notice
 electronic notice (email)
 telephone notice
 substitute notice
 Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Signature: [Signature] Date: 10/31/2008
 Contact Person, Title: Brian DuPerre Esq. Associate General Counsel
 Address: 450 Columbus Blvd., #1030-15NB, Hartford, CT 06103
 Telephone: 860-702-7095 Fax: 860-702-6570 Email: brian_duperre @ uhc . com

** Confidential – Not for External Distribution**

Fiserv Health – Affected Individuals Letter (Receiving Equifax)

Final

October 23, 2008

Fiserv Health – Affected Individuals Letter (Receiving Equifax)

<Name>

<Address Line 1>

<Address Line 2>

<City, STATE>

<Date>

Dear <NAME>,

I am writing to inform you that a laptop computer and a portable hard drive were stolen recently from a Fiserv Health employee's personal vehicle. Unfortunately, certain files saved on the stolen equipment contained some of your personal information. For details on the type of information, please see Attachment A to this letter.

Fiserv Health is a company that helps businesses and their health insurers administer employee health benefits. The company has launched an investigation into the matter, which occurred on September 25, 2008 in San Antonio, TX, and is working with local law enforcement authorities to recover the computer and portable hard drive.

The facts as determined by the company's investigation so far suggest that this was a random theft and that the personal information was not specifically targeted. The laptop was password protected and data encrypted. However, information on the portable hard drive did not have the same protections.

Fiserv Health takes this matter very seriously. As a precaution to help you detect any possible misuse of your personal information, we are offering you one year of free "Equifax Credit Watch™ Gold with 3-in-1 Monitoring," which includes identity theft insurance, fraud alerts, Equifax counselors, and routine credit reports from all three national credit bureaus. We have also enclosed further details and information on how to access this service.

In addition, we have established a dedicated hotline that you can call if you have any questions. The hotline – (888) 877-8241 – is open Monday – Friday from 9 a.m. ET to 8 p.m. ET and on weekends from 10 a.m. to 4 p.m. ET.

If, at any time, you find suspicious activity on your credit reports, please file a complaint with the FTC at www.ftc.gov/idtheft or call (877) ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible by law enforcement agencies for their investigations. It is also advisable to notify all three national credit reporting agencies should you notice any suspicious activity, as well as your local law enforcement or state Attorney General's office.

** Confidential - Not for External Distribution **

Fiserv Health - Affected Individuals Letter (Receiving Equifax)

Final

October 23, 2008

Protecting personal information is very important to Fiserv Health. We are reinforcing our existing policies and practices with employees and evaluating additional safeguards to help prevent a similar incident from occurring in the future. We deeply regret any inconvenience or concern caused by this incident.

Sincerely,

XXXXXX

** Confidential - Not for External Distribution **
Fiserv Health - Affected Individuals Letter (Receiving Equifax)
Final
October 23, 2008

ATTACHMENT A

Insert individual's specific information

** Confidential - Not for External Distribution **

Fiserv Health - Affected Individuals Letter (Receiving Equifax)

Final

October 23, 2008

INFORMATION ABOUT HOW TO MONITOR AND PROTECT YOUR CREDIT

If you do not have a subscription to a credit monitoring and protection service, we would urge you to take the steps outlined below in order to safeguard your personal information.

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling (877) 322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify it of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you see anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below:

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742

Equifax
P.O. Box 105788
Atlanta, Georgia 30348
888-766-0008

TransUnion
P.O. Box 6790
Fullerton, CA 92834
800-680-7289 or
888-909-8872

If, at any time, you find suspicious activity on your credit reports, please file a complaint with the FTC at www.ftc.gov/idtheft or call (877) ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible by law enforcement agencies for their investigations. It is also advisable to notify all three national credit reporting agencies if you notice any suspicious activity, as well as your local law enforcement or state Attorney General's office.

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and requires them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file. In addition, you should closely monitor your banking and credit account statements for suspicious activity on your existing accounts.