

February 9, 2005

I'm writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address, and Social Security number being viewed by businesses that are not allowed to access such information. We have reason to believe your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you.

Although we have been informed that disclosing too many details of the crime may hurt on-going criminal investigations, we wanted to provide you with some information related to this incident that may help you protect yourself against identity theft. First and foremost, we are actively working with the appropriate police agencies on this matter.

We believe that several individuals, posing as legitimate business customers, recently committed fraud by claiming to have a lawful purpose for accessing information about individuals, when in fact, they did not. When the fraud was discovered, access to information was discontinued and the authorities notified.

We are working with local and federal law enforcement officials to identify the people responsible for the theft of the information so they may be prosecuted for their actions. We have adjusted our procedures to help protect against a repeat event.

As information, our business customers use ChoicePoint to verify information supplied by individuals as part of a business transaction, often as part of an application for insurance, a job, or a home lease. We rely on information, including public records that are available to any citizen. This includes information created by a government agency such as a criminal history or property ownership record. We also use publicly available information, such as a published telephone number.

There are some actions, though, that only you can take to protect yourself from the misuse of information about you.

First, industry experts recommend that you place a fraud alert on your credit report by calling the toll-free fraud number of any one of the three credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

Equifax:

(800) 525-6285

Post Office Box 740241 Atlanta, GA 30374 - 0241

http://www.equifax.com

Experian:

(888) 397-3742

Post Office Box 9532

Allen, TX 75013

http://www.experian.com

TransUnion:

(800) 680-7289

Fraud Victim Assistance Division

Post Office Box 6790

Fullerton, CA 92834-6790

http://www.transunion.com

Second, when you receive your credit reports, please review them carefully. Look for inquiries you did not initiate, accounts you did not open, and unexplained debts on the accounts you opened. If there are accounts or charges you did not authorize, immediately notify the credit bureau by telephone and in writing.

You also should check to see that information such as your Social Security number, address(es), first and last names, middle initial and employers are correct. Errors in this information are often the warning signs of identity theft. Keep in mind, however, that inaccuracies in this information also may be due to simple mistakes. Nevertheless, if there are any inaccuracies in your report, whether due to fraud or error, you should also notify the credit bureau as soon as possible so the information can be investigated and, if found to be in error, corrected.

You should continue to check your credit reports frequently for the next year, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works when you request a fraud alert for the first time. If you want additional credit reports later in the year or if you want to renew the fraud alert, the three major credit bureaus require you to contact each organization separately.

Finally, if you have discovered errors or suspicious activity on your credit report, you should consider immediately contacting any credit card companies with whom you have an account and tell them that you have received this letter. You should make sure the address they have on file is your current address and that any charges on the account were made by you. If you have not already done so, you should consider adding a Personal Identification Number, or PIN, to your credit accounts. This will serve as an additional tool to protect your account and help the credit card company ensure they are only processing changes authorized by you.

We have set up a toll-free number to accept calls from consumers with questions and to provide any additional advice and support we can. To speak to someone about the information in this letter, please call 1-877-547-2518 between the hours of 6:00 am and 7:30 pm Pacific time, Monday through Friday. We hope this information is helpful to you and regret any inconvenience this may cause you.

Sincerely,

J. Michael de Janes Chief Privacy Officer