

ANHEUSER



BUSCH

Companies

Lisa A. Joley
VICE PRESIDENT
AND GENERAL COUNSEL

July 21, 2008

Attorney General Kelly A. Ayotte
Office of Attorney General
33 Capitol Street
Concord, NH 03301

Dear General Ayotte:

I am writing this letter in accordance with your state's law requiring notification to you in cases of data security breaches. A burglary occurred at an Anheuser-Busch Companies, Inc. ("A-BC") office in Sunset Hills, Missouri, sometime between the evening of June 6, 2008 and the morning of June 9, 2008. Two other business tenants in the same office building were burglarized as well. Laptop computers were stolen from each business, including the A-BC office. The information contained on one of the A-BC stolen laptops contained personal information of approximately 2,250 of your state's residents, including their name, address and phone number, social security number, date of birth, ethnicity and marital status. The theft was reported to the police and A-BC is cooperating with their investigation.

In addition, the information contained on the A-BC stolen laptops contained information relating to the services received from the A-BC Employee Assistance Program ("EAP") on approximately 750 of your state's residents, including EAP case notes and assessments, the names of the providers to whom the individuals were referred, and the treatment plans recommended by the providers.

The stolen A-BC laptops were password protected and the information was encrypted. At this time, there is no evidence that this incident has led to fraudulent credit applications or other identity theft crimes. We have taken this issue very seriously by implementing additional quality controls to avoid similar incidents in the future. These controls include enhanced security measures that limit remote use to specifically designated individuals. We are sending notice letters of the breach to all individuals whose names were in the data base. We will begin the process of mailing the notices to affected individuals the week of July 21, 2008. Because we are committed to assisting the affected individuals, we have arranged with Equifax Personal Solutions to help them protect their identity and monitor credit information at no cost to them for one year and have provided enrollment steps.

We are also alerting the affected individuals that they may consider placing an initial fraud alert on their credit file that would let creditors know to contact them before opening new accounts or making changes to existing accounts. Individuals wishing to place a fraud alert on their credit file are being advised to visit www.fraudalerts.equifax.com or contact Equifax's auto fraud line at 1-877-478-7625 and follow the simple prompts. We have noted, however, that the Federal Trade Commission recommends placing a fraud alert on a credit file ONLY in the event that the person has been an actual victim of identity theft. The process is free of charge and available to affected individuals if they believe they are at risk of identity theft. Equifax may investigate an affected individual's request for an alert, and we will provide the credit bureau with any assistance necessary. Once Equifax places a fraud alert on the individual's credit file, it will notify the other credit bureaus, which will also place an alert on the individual's credit record.

Attorney General Kelly A. Ayotte
July 21, 2008
Page 2

In addition, affected individuals are being advised that about two-thirds of the states have laws that enable individuals to place a "security freeze" on their credit reports. This is stronger than a fraud alert because it prevents anyone from accessing an individual's credit file for any reason unless the individual instructs the credit bureaus to unfreeze his/her report. Affected individuals are being provided a link for a list of the states where a security freeze is available (www.consumersunion.org/campaigns/financialprivacynow) and are also being advised that a security freeze is an extreme remedy and is recommended ONLY for certain people who have been the actual victim of identity theft. The security freeze is free to victims of identity theft in most states. Non-victims who wish to activate the security freeze for prevention must pay a fee in most states. Some states make the security freeze available only to identity theft victims.

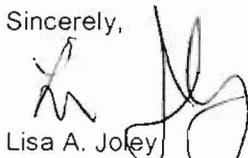
The affected individuals are also being advised that they may obtain more information about fraud alerts, security freezes and other aspects of protecting themselves against identity theft, by visiting www.fightidentitytheft.com. They are also being provided the contact information for the consumer reporting agencies listed below and advised they may obtain a free copy of their credit report by visiting www.annualcreditreport.com or by calling toll free 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. The three credit bureaus are:

Equifax	Experian	TransUnion
877-478-7625	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Lastly, we have provided notice of the incident to the above three credit reporting agencies. Included in that notice is the total number of affected individuals.

I have enclosed a copy of each notice that will be sent to residents of the state of New Hampshire for your reference.

Sincerely,



Lisa A. Joley
Vice President and General Counsel
Anheuser-Busch Companies, Inc.

[DATE]

[NAME]

[ADDRESS]

[ADDRESS]

Dear [NAME]:

This is to inform you of a recent incident involving records containing information about you.

A burglary occurred at an Anheuser-Busch Companies, Inc. (A-BC) office sometime between the evening of Friday, June 6, 2008 and the morning of Monday, June 9, 2008. Two other business tenants in the same office building were also burglarized. Laptop computers were stolen from each business, including the A-BC office. One of the stolen A-BC laptops contained password protected, encrypted data which included your name, home address and phone number, social security number, date of birth, ethnicity and marital status. In addition, if you have utilized the Employee Assistance Program (EAP) in the past, the information contained on the A-BC stolen laptops also related to the individual services provided by the EAP, including EAP case notes and assessments, the names of the providers to whom you were referred, and the treatment plans recommended by the providers. The theft was reported to the police and A-BC is cooperating fully with their investigation.

Again, the stolen laptop computers were password protected and the information was encrypted. At this time, there is no evidence that the theft of employee data has resulted in any unauthorized disclosure, fraudulent credit applications or other identity theft crimes. Nonetheless, you should be vigilant by monitoring your account statements and reviewing free credit reports (as described below). If you suspect any of your information is improperly used, you should report this to your local police department and your state attorney general's office. In addition, please notify Equifax as well. We have taken this issue very seriously and have assembled resources and implemented steps to address the potential for improper use of the stolen information.

First, we have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you if you enroll by October 31, 2008. The Equifax Credit Watch™ Silver identity theft protection product will be provided to you at no cost for one year. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two major credit reporting agencies.

About Equifax Credit Watch™ Silver:

Equifax Credit Watch™ Silver will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. Equifax Credit Watch™ Silver provides you with the following benefits:

- Comprehensive monitoring of your Equifax credit file with e-mail notifications of key changes
- Wireless alerts and customizable alerts available
- One Free Equifax Credit Report™
- Up to \$2,500 Identity Theft Insurance with \$250 deductible (certain limitations and exclusions apply) †
- Knowledgeable Customer Care 24 hours a day, 7 days a week

How to Enroll in Equifax Credit Watch™ Silver:

Equifax has a simple Internet-based verification and enrollment process. To enroll, visit www.myservices.equifax.com/silver by October 31, 2008, and follow these steps:

1. Consumer Information: Complete the form with your contact information (name, address and e-mail address) and click "Continue." The information is provided in a secured environment.
2. Identity Verification: Complete the form with your Social Security Number, date of birth, telephone numbers, create a User Name and Password, agree to the Terms of Use and click "Continue." The system will ask you up to two security questions to verify your identity.
3. Payment Information: During the "check out" process, enter <XXXXX> in the "Enter Promotion Code" box (include the dash but no spaces.) After entering your code, click "Apply Code" and then "Submit Order" at the bottom of the page. This code eliminates the need to provide a credit card number for payment.
4. Order Confirmation: – Click "View My Product" to access your Equifax Credit Report.

Additional Options:

Second, you may also consider placing an initial fraud alert on your credit file.

- A fraud alert lets creditors know to contact you before opening new accounts or making changes to existing accounts.
- The Federal Trade Commission recommends placing a fraud alert on your credit file ONLY in the event you have been an actual victim of identity theft. Fraud alerts can cause difficulties if you attempt to obtain new credit yourself.
- The process is free of charge and available if you believe you are at risk of identity theft. Once Equifax places a fraud alert on your credit file, it will notify the other credit bureaus, which will also place an alert on your credit record.
- To place a fraud alert on your credit file, visit www.fraudalerts.equifax.com or you may contact Equifax's automated fraud line at 1-877-478-7625 and follow the simple prompts.

Third, you may also consider setting a security freeze on your credit report in those states where it is available.

- Our research shows about two-thirds of the states have laws that enable individuals to place a security freeze on their credit reports.
- A security freeze is stronger than a fraud alert because it prevents anyone from accessing your credit file for any reason unless you instruct the credit bureaus to unfreeze your report.
- Be aware a security freeze is an extreme remedy and is recommended ONLY for certain people who have been the actual victim of identity theft. If your identity is stolen, and your identity thief is aggressive and gives no indication of ceasing to use your identity to obtain credit, consider using the security freeze to reduce access to your credit file.
- The security freeze is free to victims of identity theft in most states. Non-victims who wish to activate the security freeze for prevention must pay a fee in most states. Some states make the security freeze available only to identity theft victims.
- For a list of the states where a security freeze is available, visit www.consumersunion.org/campaigns/financialprivacynow.

Important Resources:

- For more information about fraud alerts, security freezes and other aspects of protecting yourself against identity theft, please visit www.fightidentitytheft.com.
- To obtain a free copy of your credit report, you may visit www.annualcreditreport.com online, or call toll free 1-877-322-8228. Hearing impaired consumers can access TDD service at 1-877-730-4104. The three credit bureaus are:

Equifax	Experian	TransUnion
1-877-478-7625	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- For more information about steps you can take to avoid identity theft, you may contact the Federal Trade Commission at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.ftc.gov/>
1-877-382-4357/ TTY: 1-866-653-4261

Finally, we have implemented additional controls to avoid a similar future incident. These controls include enhanced security measures which limit use to select authorized personnel.

We sincerely apologize this incident has occurred. The action steps we are taking and suggesting you take are preventive. If you have any questions about this incident, or if you find any of your information is improperly used, please call the Anheuser-Busch helpline provided by Equifax at 1-800-913-4502, Monday through Friday from 8:00 a.m. to 12:00 a.m., Eastern Standard Time.

Sincerely,

James G. Brickey
Vice President – Human Resources & Total Rewards
Anheuser-Busch, Inc.

† Identity Fraud 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 our underwriting qualifications and state regulators. Coverage not available for residents of New York.

[DATE]

[NAME]

[ADDRESS]

[ADDRESS]

Dear [NAME]:

This is to inform you of a recent incident involving records containing information about you.

A burglary occurred at an Anheuser-Busch Companies, Inc. (A-BC) office sometime between the evening of Friday, June 6, 2008 and the morning of Monday, June 9, 2008. Two other business tenants in the same office building were also burglarized. Laptop computers were stolen from each business, including the A-BC office. One of the stolen A-BC laptops contained password protected, encrypted data which included your name, home address and phone number, social security number, date of birth, ethnicity and marital status. In addition, if you have utilized the Employee Assistance Program (EAP) in the past, the information contained on the A-BC stolen laptops also related to the individual services provided by the EAP, including EAP case notes and assessments, the names of the providers to whom you were referred, and the treatment plans recommended by the providers. The theft was reported to the police and A-BC is cooperating fully with their investigation.

Again, the stolen laptop computers were password protected and the information was encrypted. At this time, there is no evidence that the theft of employee data has resulted in any unauthorized disclosure, fraudulent credit applications or other identity theft crimes. Nonetheless, you should be vigilant by monitoring your account statements and reviewing free credit reports (as described below). If you suspect any of your information is improperly used, you should report this to your local police department and your state attorney general's office. In addition, please notify Equifax as well. We have taken this issue very seriously and have assembled resources and implemented steps to address the potential for improper use of the stolen information.

First, we have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you if you enroll by October 31, 2008. The Equifax Credit Watch™ Silver identity theft protection product will be provided to you at no cost for one year. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two major credit reporting agencies.

About Equifax Credit Watch™ Silver:

Equifax Credit Watch™ Silver will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. Equifax Credit Watch™ Silver provides you with the following benefits:

- Comprehensive monitoring of your Equifax credit file with e-mail notifications of key changes
- Wireless alerts and customizable alerts available
- One Free Equifax Credit Report™
- Up to \$2,500 Identity Theft Insurance with \$250 deductible (certain limitations and exclusions apply) †
- Knowledgeable Customer Care 24 hours a day, 7 days a week

Important Resources:

- For more information about fraud alerts, security freezes and other aspects of protecting yourself against identity theft, please visit www.fightidentitytheft.com.
- To obtain a free copy of your credit report, you may visit www.annualcreditreport.com online, or call toll free 1-877-322-8228. Hearing impaired consumers can access TDD service at 1-877-730-4104. The three credit bureaus are:

Equifax	Experian	TransUnion
1-877-478-7625	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- For more information about steps you can take to avoid identity theft, you may contact the Federal Trade Commission at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.ftc.gov/>
1-877-382-4357/ TTY: 1-866-653-4261

Finally, we have implemented additional controls to avoid a similar future incident. These controls include enhanced security measures which limit use to select authorized personnel.

We sincerely apologize this incident has occurred. The action steps we are taking and suggesting you take are preventive. If you have any questions about this incident, or if you find any of your information is improperly used, please call the Anheuser-Busch helpline provided by Equifax at 1-800-913-4502, Monday through Friday from 8:00 a.m. to 12:00 a.m., Eastern Standard Time.

Sincerely,

James G. Brickey
Vice President – Human Resources & Total Rewards
Anheuser-Busch, Inc.

† Identity Fraud 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 our underwriting qualifications and state regulators. Coverage not available for residents of New York.

[DATE]

[NAME]

[ADDRESS]

[ADDRESS]

Dear [NAME]:

This is to inform you of a recent incident involving records containing information about you.

A burglary occurred at an Anheuser-Busch Companies, Inc. (A-BC) office sometime between the evening of Friday, June 6, 2008 and the morning of Monday, June 9, 2008. Two other business tenants in the same office building were also burglarized. Laptop computers were stolen from each business, including the A-BC office. One of the stolen A-BC laptops contained password protected, encrypted data which included your name, home address and phone number, social security number, date of birth, ethnicity and marital status. In addition, if you have utilized the Employee Assistance Program (EAP) in the past, the information contained on the A-BC stolen laptops also related to the individual services provided by the EAP, including EAP case notes and assessments, the names of the providers to whom you were referred, and the treatment plans recommended by the providers. The theft was reported to the police and A-BC is cooperating fully with their investigation.

Again, the stolen laptop computers were password protected and the information was encrypted. At this time, there is no evidence that the theft of employee data has resulted in any unauthorized disclosure, fraudulent credit applications or other identity theft crimes. If you suspect any of your information is improperly used, you should report this to your local police department and your state attorney general's office. In addition, please notify Equifax as well. We have taken this issue very seriously and have assembled resources and implemented steps to address the potential for improper use of the stolen information.

Our records indicate that you are a minor and therefore do not yet have credit. If our records are inaccurate, please contact Equifax at 1-800-913-4502. Equifax does not provide credit monitoring services for minors and therefore such services cannot be offered to you. Please note however that Equifax takes steps to ensure that their database does not contain credit files on minor children. If a creditor sends them information on a consumer and the birth date equals less than 18 years of age then they will reject the data so that no credit report is created.

However, if a parent or guardian is interested in confirming whether an Equifax credit file exists for their minor they can take the following step:

Parents/guardians are asked to send Equifax a copy of the minor child's birth certificate and a copy of a social security number card or letter/form from the Social Security Administration along with a letter explaining that they may be a victim of identity theft (sample letter is attached). Additionally, please provide a copy of your driver's license or other government-issued proof of your identity, which includes your current address. Please send this information to the following address:

Equifax Information Services
P.O. Box 105139
Atlanta, Georgia 30374

Once Equifax receives this information they will perform a search of their data base for the minors SSN number. If they do NOT find a match then they will inform the parent or guardian in writing that the SSN number was not found. If they do find a match then they will take the necessary steps to protect the minor's social security number by placing a 7 year fraud alert on that number and will also inform the parent or guardian in writing of the steps taken.

Finally, we have implemented additional controls to avoid a similar future incident. These controls include enhanced security measures which limit use to select authorized personnel.

We sincerely apologize this incident has occurred. The action steps we are taking and suggesting you take are preventive. If you have any questions about this incident, or if you find any of your information is improperly used, please call the Anheuser-Busch helpline provided by Equifax at 1-800-913-4502, Monday through Friday from 8:00 a.m. to 12:00 a.m., Eastern Standard Time.

Sincerely,

James G. Brickey
Vice President – Human Resources & Total Rewards
Anheuser-Busch, Inc.

Sample Letter

Equifax Information Services
P.O. Box 105139
Atlanta, GA 30348

RE: Minor SSN Inquiry

Dear Equifax:

My Child (_____) may have been a fraud victim due to a resent data breach with "company name".

Please initiate a research request regarding the possible fraudulent use of my child's social security number. Enclosed are the following documents necessary for this research:

- A copy of the child's birth certificate.
- A copy of the child's social security card or a document from the Social Security Administration that shows the child's social security number.
- Parent/guardian identification

Thank you.

Minor Child's Parent/Guardian name and address phone and email.