



Date

[Insert contact name]
[Insert address line one]
[Insert address line two]

Dear [Insert contact name]:

I am writing to inform you of a matter that the Cigna Enterprise Privacy Office was made aware of on March 27, 2012. On March 23, 2012, in violation of Cigna corporate policies, a Cigna employee emailed an unencrypted document containing Cigna Dental customers' first names and social security numbers to her home email address and to the email address of her son. The document was created by Cigna for internal use by our Dental Customer Service Agents. It included your first name and social security number, but it did not contain any other personal information about you (such as your address or health information).

At Cigna, we take this type of policy violation very seriously. The employee indicated that she had emailed the document with the intention of reviewing it at home, with the assistance of her son, so that she could identify the Cigna customers who had been assigned to her for follow-up telephone calls. The employee confirmed, in writing, that she destroyed the document, retained no copies of it, and that it was not shared with anyone else. We have received confirmation from the son as well, that he destroyed the document, retained no copies of it, and that it was not shared with anyone else. The employee's position with Cigna was terminated on March 29.

Cigna is already taking steps to prevent this type of situation from recurring. The document forwarded by the former employee is no longer being produced for internal distribution to Cigna's Customer Service Agents as this information is accessible through other, secure means. Additional automatic preventive safeguards are being enhanced to help minimize the potential for future occurrences of this type of policy violation. Cigna is also retraining its workforce on privacy and information protection regulations and corporate policies in May and June.

Based on the facts of this situation, Cigna does not believe that there is significant risk that your personal information will be misused. However, we understand and expect that this disclosure of your personal information may cause you to be concerned. Therefore, we have arranged for you to take advantage of a **free two (2) year subscription for credit monitoring** (Equifax Credit Watch™ Gold). Upon enrollment, this comprehensive credit file monitoring and automated alert service will notify you of key changes to your credit report, including fraudulent activity, new inquiries and new accounts added to your credit reports. Specifically, this service provides for:

- Comprehensive credit-file monitoring of your Equifax credit report with daily notification of key changes to your credit file;
- Wireless alerts and customizable alerts available;
- Unlimited access to your Equifax Credit Report;
- \$25,000 in identity theft protection with \$0 deductible, at no additional cost to you (certain limitations and exclusions may apply);
- Live agent Customer Service 24 hours a day, seven days a week to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and to help you initiate an investigation of inaccurate information.

To take advantage of this credit monitoring program, please call 1-800-394-3598 between 9am and 9pm EST and we will provide you with a promotion code to register with Equifax.

Once you receive your credit report, review it carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Additionally, look for personal information that is not accurate, such as your home address and social security number. If you see anything you don't understand, call the credit agency at the telephone number on the report. If you do find suspicious activity on your credit report, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

We also recommend that you take the following steps to protect yourself from misuse of your personal information:

- Set a fraud alert in your credit file. The fraud alert tells creditors that you want to be contacted before new accounts are opened. The fraud alert and credit report are available free of charge by contacting one of the credit reporting agencies listed below and mentioning this incident:

Equifax	TransUnion	Experian
P.O. Box 105069 Atlanta, GA 30374	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834	P.O. Box 9532 Allen, TX 75013
1-800-525-6285	1-800-680-7289	1-888-397-3742
www.equifax.com	www.transunion.com	www.experian.com

- Review the FTC's website for information regarding identity theft at www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also write to the FTC at Federal Trade Commission Consumer Response Center at 600 Pennsylvania Avenue, NW Washington, DC 20580.

- Consider placing 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 file at the credit reporting agencies without your consent. There may be fees for placing, lifting or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each credit reporting agency individually.* For more information on security freezes, you may contact the three national credit reporting agencies or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit reporting agencies for more information.

We regret that this incident occurred and that it has impacted you. Cigna is committed to protecting the personal information of all those we serve, and we apologize for your inconvenience. If you have any questions, please contact us at 1-800-394-3598 between 9am and 9pm EST.

Sincerely,

A handwritten signature in cursive script that reads "Barbara R. Billman".

Barbara Billman
Cigna Privacy Office