blue of california

John Doe
1234 Main Street
Huntington Beach, CA 92646

June __, 2015

Dear Mr. Doe:

I am writing to advise you of Blue Shield of California's ("Blue Shield") unintentional, unauthorized disclosure of your personal information (your "Protected Health Information" or "PHI"). We have no reason to believe that your PHI has been inappropriately used or further disclosed. However, we want to make you aware of the circumstances that led to the disclosure, as well as the steps Blue Shield has taken to address the matter. I apologize for any concern or inconvenience this may cause you.

Between May 9, 2015 and May 18, 2015, your PHI may have been disclosed to an otherwise authorized user of the secure website that Blue Shield maintains for use by our group health benefit plan administrators and brokers. Authorized users may access the website (the "Website") to manage information about their own health benefit plan members.

As the (unintended) result of a computer code update Blue Shield made to the Website on May 9, three users who logged into their own Website accounts simultaneously with (at the exact same time as) another user were able to view member information associated with the other user's Website account. This issue was reported to the Blue Shield Privacy Office on May 18. The Website was promptly taken off line to identify and correct the problem. The Website's faulty code was identified and corrected and the Website was returned to service on May 19. Our investigation revealed that this was the result of human error on the part of Blue Shield staff members, and the matter was not reported to law enforcement authorities for further investigation.

Your PHI that was accessible to a Website user who was not authorized to view it included your first and last name, Social Security Number, Blue Shield identification number, date of birth, and home address. None of your financial information was made available as a result of this incident. The users who had unauthorized access to PHI as a result of this incident have confirmed that they did not retain copies, they did not use or further disclose your PHI, and that they have deleted, returned to Blue Shield, and/or securely destroyed all records of the PHI they accessed without authorization.

Blue Shield is committed to maintaining your privacy and takes this incident seriously. To prevent this type of incident in the future, we have implemented additional code review which will help us to identify this type of vulnerability before the code is placed into use.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps:

1. **Ensure That You Enroll By:** 9/5/15 (Your code will not work after this date.)
2. **Visit the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. **Provide Your Activation Code:** _____

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: _____.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE™:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
    - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance** (subject to availability)**:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

We recommend that you always remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, call the FTC, at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your

credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Experian (888) 397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

We sincerely apologize and regret any inconvenience this may cause you. Should you have questions regarding this matter and/or the protections available to you, please do not hesitate to contact us at 1-888-263-2499.

Sincerely,

Hope H. Scott, Esq., CIPP/US
Chief Privacy Official
Blue Shield of California