To Whom It May Concern:

Blue Shield of Californica ("BSC") would like to notify the Maryland Attorney General's Office that on March 22, 2023, BSC was notified that a former Business Associate, HealthPlan Services ("HPS"), was a victim of a malware attack on June 23, 2022, that affected its network and resulted in an unauthorized party accessing and/or acquiring certain files or folders from portions of its network. BSC systems were not impacted by this event.

Upon detecting the incident, HPS commenced an investigation, contained its network and alerted law enforcement. As part of their investigation, HPS engaged cybersecurity professionals to identify the extent of the activity and what, if any, Protected Health Information (PHI) may have been accessed and/or acquired by the unauthorized party. Following the forensic investigation and manual document review, on March 21, 2023, HPS determined that BSC member Protected Health Information was involved in the incident.

HPS advised that the following actions were taken to prevent a security incident from occurring again:

- CrowdStrike, Tanium, Mcafee deployed to all systems.
- Email migrated to O365 which utilizes a SEG, DMARC, DKIM, and SPF protection.
- All credentials pertaining to privileged accounts are stored securely within the Cyberark PAM vault.
- In addition to requiring RSA MFA to a jump box to access DMZ; all critical servers require a secondary MFA utilizing DUO.
- All HPS users attended mandatory FBI cybersecurity training with an emphasis on email phishing.
- End user phishing test frequency increased and corrective actions strengthen for non-compliance.
- Security awareness notifications routinely sent to WHPS users to help emphasize the importance of strong security practices.
- Implemented Zero Trust Security Framework.

Three Maryland residents were impacted by this security incident and the amount of PHI that may have been accessed and/or acquired varies by member. The PHI that may have been involved included: Date of birth, Social Security Number, insurance information, and medical record number.

Legal counsel representing HPS advised that they would make the following notifications on behalf of BSC: Member, Office for Civil Rights (OCR), applicable state attorney generals, substitute notice, and media notice; however, legal counsel believed there was an exemption to notify the Maryland Attorney General's Office, which BSC disagreed upon. After BSC's multiple requests to notify the Maryland Attorney General's Office on our behalf, HPS failed to make the notification, which caused this delay in reporting. HPS made member notification and OCR notification on April 28, 2023, and a sample copy of the letter provided to consumers is attached.

Should you have any questions, please feel free to let me know.

Regards,

Gina Dayao, CHPC
Consultant, Privacy Office
601 12th Street, Oakland, CA 94607
Privacy Office: 888-266-8080| Work: 916-566-5482
Fax: 800-201-9020

HealthPlan Services, Inc.

To Enroll, Please Call:
[PHONE]
Or Visit:
[WEBSITE]
Enrollment Code: <<XXXXXXXX>>

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Date>>

<<Variable Header>>

Dear <<First>> <<Last>>:

We are writing with important information regarding a data security incident that may have affected your Protected Health Information. HealthPlan Services ("HPS") provides certain technology-based services for <<carrier>>, which requires access to certain member Protected Health Information. The privacy and security of the information we maintain is of the utmost importance to HPS. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

HPS detected that some elements within our network had been affected by malware, and as a result the unauthorized party accessed and/or acquired certain files or folders from portions of our network on June 23, 2022.

What We Are Doing

Upon detecting the incident, HPS commenced an immediate and thorough investigation, contained the network and alerted law enforcement. As part of our investigation, HPS engaged leading cybersecurity professionals to identify the extent of the activity and what, if any, member Protected Health Information may have been accessed and/or acquired by the unauthorized party. After a thorough and detailed forensic investigation and comprehensive manual document review, on March 21, 2023, HPS determined that your Protected Health Information may have been involved in the incident. Upon request HPS subsequently moved to notify you about this incident and provide you with information to protect your personal and health information.

What Information Was Involved?

The information potentially involved includes your full name and <<PHI involved>>.

What You Can Do

To protect you from the potential misuse of your information, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary 12-month membership, please see the additional information provided in this letter.

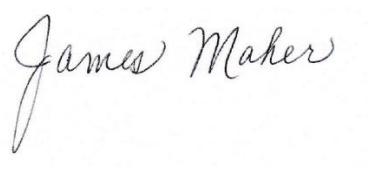
This letter also provides other precautionary measures you can take to protect your information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

HPS values your privacy and deeply regrets that this incident has occurred. We take the security of your information very seriously and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [PHONE]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 9AM to 9PM Eastern time, excluding holidays.

Sincerely,



President and CEO
HealthPlan Services, Inc.

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Go to [WEBSITE] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is [**DATE**]. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any

accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (June 23, 2022) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.