Date

«Individuals\_First\_Name» «Individuals\_Last\_Name»

«Individuals\_Street\_Address»

«Individuals\_City», «Individuals\_State» «Individuals\_Zip\_Code»

Re: **NOTICE OF DATA BREACH**

**PLEASE READ CAREFULLY**

Dear «Individuals\_First\_Name» «Individuals\_Last\_Name»:

Blue Cross and Blue Shield of Illinois (BCBIL) is providing this letter because of your past or current health insurance coverage with BCBSIL. It is being sent to provide you with specific details about a recent incident involving your Protected Health Information (PHI) as required under the law.

***What Happened:*** On 06/23/2023 we became aware that your PHI was accessed by an unauthorized party on 06/21/2023 at a vendor of TMG Health (TMG). TMG provides third party administrative services to Medicare enrollees of HCSC Insurance Services Company (HISC). HISC is contracted with the Centers for Medicare and Medicaid Services (CMS) to offer this product.

***What Information Was Involved:*** The information that was disclosed included your name, address, email address, phone number, date of birth, Social Security Number, Claim number, bank account number and medical service information. We have investigated the incident and determined that due to the unauthorized access by a bad actor, your information may have been disclosed to the wrong individual.

***What We Are Doing:*** In order to minimize any harm, TMG is working closely with the vendor to ensure systems are updated to block these activities and prevent disclosures of this nature from occurring in the future. TMG is committed to maintaining the privacy and security of your information and is taking this incident very seriously. Our vendor has notified law enforcement to mitigate this situation as best as possible.

***What You Can Do:*** BCBSIL takes the confidentiality of members’ data very seriously. We have no reason to believe that anyone has accessed or misused your information. However, we want to make you aware of steps you may take to guard against identity theft or fraud. If you receive or access explanation of benefits statements (EOBs) from BCBSIL, we recommend that you regularly review these statements. If you see any service that you did not receive, please call us at the number found on the statement or on the back of your member identification (ID) card. If you do not receive or access EOBs, contact your provider or plan and request that they send you a statement following the provision of any services under your name and ID number. Please review the enclosed Information about Identity Theft Protection.

**What we are doing to protect your information:** Additionally, to assist in protecting you from any potential identity theft, we are offering you one year of complimentary [credit/identity theft/dark web monitoring service through IDX’s [Name of Product]. You have [\*\*] days from the date of this letter to activate the free credit monitoring service by using the following activation code: [\*\*\*]. This code is unique for your use and should not be shared. You can enroll by calling [8XX-XXX-XXXX] or you can visit [\_\_\_@\_\_\_\_]. To learn more about what is included with these services please review the enclosure.

Due to privacy laws, we cannot register you directly.

***What you can do to protect your information*:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the final page of this letter.

***For More Information:*** If you believe that your PHI has been misused or have any questions regarding this letter, please call the toll-free number listed on your member ID card. A representative is available to assist you.

Sincerely,

Privacy Office

Blue Cross and Blue Shield of Illinois

Enclosures

|  |  |
| --- | --- |
|  |  |

**Additional Information**

You should always remain vigilant, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your Attorney General, 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 website, at www.consumer.gov/idtheft, or 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 the federal Fair Credit Reporting Act (“FCRA”), 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 Experian TransUnion

(800) 685-1111 (888) 397-3742 (888) 909-8872

P.O. Box 740241 P.O. Box 9701 Fraud Victim Assistance Division

Atlanta, GA 30374-0241 Allen, TX 75013 P.O. Box 2000

Equifax.com/personal/ Experian.com/help Chester, PA 19022

credit-report-services TransUnion.com/credit-help

In addition, you may obtain additional 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. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

Equifax – (800) 685-1111

Experian – (888) 397-3742

TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

Close-up of a medical form

Description automatically generated

A close-up of a document

Description automatically generated