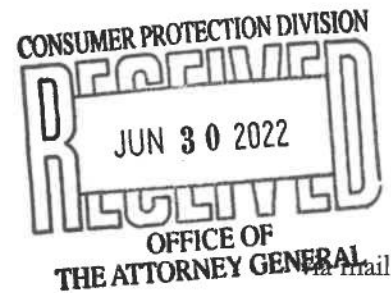


Stacy Harper
Direct Dial: 913.317.6045
sharper@spencerfane.com

June 10, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 Saint Paul Place
Baltimore, MD 21202



Re: Notification of Data Security Incident

Dear Office of the Attorney General:

We are writing on behalf of our client, Premera Blue Cross, in connection with the recent data security incident described below. Premera Blue Cross is a healthcare insurance plan with a principal address of 7001 220th St SW, Mountlake Terrace, Washington 98043.

On May 17, 2022, the prescription and pharmacy vendor of Premera Blue Cross, Express Scripts, notified Premera of a security incident that impacted the Express Scripts mobile application in late April of 2022. Because some of Premera's customers received prescription(s)/pharmacy services through Express Scripts, and have a registered account on their mobile app, the information of some Premera customers, which include four Maryland residents, may have been exposed due to this incident. Per Express Scripts, on April 30, 2022, Express Scripts identified an irregular volume of login attempts for its mobile app. Upon discovery, Express Scripts locked all potentially compromised accounts to prevent further access, forced a password reset, and temporarily shut down the mobile app for further investigation. Additional monitoring, blocking, and preventive controls were put in place to detect and respond to any additional unauthorized activity. Express Scripts believes the pattern of unusual activity on the mobile app is indicative of an automated "credential stuffing" attack.

The information that could have been compromised by this incident included names and up to two years of your prescription drug history, including medication name(s), prescription number(s), dosage(s), pharmacy name(s), physician name(s), and physician(s) contact information.

Express Scripts is providing free credit monitoring services as well as a customer service hotline that can be utilized for questions regarding this incident.

Notification letters will be mailed to affected individuals on June 15, 2022. A sample copy of the notice that the Maryland residents will receive is enclosed.

Respectfully,
Spencer Fane, LLP

Stacy Harper, Partner

Enclosure: Notice of Data Breach

<First Name> <Last Name>
<Mailing Address Line 1> <Mailing Address Line 2>
<City>, <ST> <Zip Code>

<Date>

Dear <First Name> <Last Name>,

Premera Blue Cross takes the privacy and security of our members' information very seriously. Regrettably, we are writing to inform you of a recent privacy incident involving Premera's prescription and pharmacy vendor, Express Scripts, which may have impacted some of your information.

What happened	On May 17, 2022, Express Scripts notified Premera of a security incident that impacted their mobile application in late April. Since you have received prescription(s)/pharmacy services through Express Scripts, and have a registered account on their mobile app, some of your information may have been exposed due to this incident. This notice explains the incident, outlines the measures taken in response, and describes the steps you can take to safeguard your information.
What you need to know	Per Express Scripts, on April 30, 2022, Express Scripts identified an irregular volume of login attempts for its mobile app. Upon discovery, Express Scripts locked all potentially compromised accounts to prevent further access, forced a password reset, and temporarily shut down the mobile app for further investigation. Additional monitoring, blocking, and preventive controls were also put in place to detect and respond to any additional unauthorized activity. Express Scripts believes the pattern of unusual activity on the mobile app is indicative of an automated "credential stuffing" attack.

	Credential stuffing typically involves an unauthorized user obtaining account credentials (usernames and/or email addresses and the corresponding passwords) from other, unrelated breaches in attempt to gain access to other sites (in this case, the Express Scripts mobile app), knowing that many individuals tend to reuse the same credentials for multiple accounts. Based on Express Scripts' forensic investigation, they determined that over 99% of the credentials used in the attack had been compromised through large, unrelated public breaches. These other breaches resulted in credentials being leaked and publicly available on the internet. On May 13, 2022, after extensive and complex research, and with the help of a third-party incident response firm, Express Scripts was able to identify members whose information may have been accessible to the perpetrators. The incident impacted less than .01% of Express Scripts' member population. The Federal Bureau of Investigation (FBI) was notified of this incident on May 5, 2022. The investigation is still ongoing and Express Scripts, along with their third-party intelligence vendor and the FBI, have not identified the person or entity responsible for this attack. Express Scripts advised that they will continue to monitor the dark web and other channels for potential security threats. Express Scripts has not detected or reported any additional threats at this time. Express Scripts will provide free credit monitoring services as well as a customer service hotline that can be utilized for questions regarding this incident. Additional details on these services are provided below.
What information could have been viewed?	It is unknown at this time if the unauthorized third party acquired or viewed any of your information. The information that could have been compromised by this incident included your name and up to two years of your prescription drug history, including medication name(s), prescription number(s), dosage(s), pharmacy name(s), physician name(s), and physician(s) contact information. It's possible some of the prescription and physician information is related to sensitive services. Your Social Security number was not exposed or compromised.

How will this be prevented in the future?

In response to this security incident, Express Scripts has taken measures to prevent this from occurring again, including the following:

- Express Scripts has expedited the implementation of mandatory multifactor authentication capabilities on the Express Scripts mobile app. Express Scripts targets this work to be completed in the third quarter of 2022.
- Express Scripts has implemented a reputable third-party security solution that prevents large-scale fraud with account takeover protection. This product monitors Express Scripts' apps 24 hours a day, 7 days a week, and detects and blocks any "bot" activity targeting Express Scripts' mobile app and website.
- Additional enhancements have been made to the mobile app, including blocking device characteristics at the network infrastructure level, deploying a new network-based technology to monitor and mitigate anomalous or potentially suspicious activity targeting the app, and updating the internal threshold monitoring tools to further limit the number of login attempts permitted for a specific IP address (since threat actors will often send bulk attacks from a limited number of IP addresses).
- Additionally, Express Scripts' threat Intelligence teams have increased monitoring of the dark web for chatter related to the sale of Express Scripts credentials.

Out of an abundance of caution, Premiera reset your member login account on www.premiera.com upon learning of this incident.

Do I need to do anything in response to this notice?

Express Scripts identified your credentials used on their mobile app as likely to be compromised. Therefore, we highly encourage you to review and update any additional accounts that have the same or similar credentials.

Express Scripts advised that they locked all accounts that were identified as potentially accessed in the attack, so your account password will need to be reset. We strongly recommend that you create a unique username and password combination that is only used to access your Express Scripts account. In addition, pending the availability of multifactor authentication in the near future, we recommend that you enable biometric authentication on the Express Scripts mobile app.

To log in to your Express Scripts mobile app, you will need to reset your password and provide additional authentication information by accessing a link that was sent to your email address on file with Express Scripts.

Express Scripts reiterated that it is unknown if any of your information exposed in this incident has been accessed or misused in any way. However, please note the following additional actions being taken, and recommended steps:

- Express Scripts is providing a 12-month free credit monitoring service through Equifax Complete Premier. We suggest you take advantage of this opportunity by following the included enrollment instructions.
- We also recommend that you closely review your Express Scripts and Premiera accounts and history for any errors or irregularities. If you do find errors or irregularities, please immediately contact Premiera at the number below.

Lastly, Express Scripts has a helpline available to assist with additional questions you may have regarding this incident. Representatives will be available 24/7. Please call the helpline at **877-463-0152**

We sincerely apologize for any inconvenience or concern this situation may cause. Premiera is committed to keeping your information secure. If you have questions, please call Premiera customer service at (800)676-1411, TTY: 711, Monday through Friday, 5am – 8pm, Pacific Time.

Sincerely,



Chris Brandt
Privacy Officer
Premera Blue Cross



<First Name> <Last Name>
Enter your Activation Code: <Activation Code>
Enrollment Deadline: <Expiration Date>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <Activation Code> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Discrimination is Against the Law

Premera Blue Cross (Premera) complies with applicable Federal and Washington state civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, sex, gender identity, or sexual orientation. Premera does not exclude people or treat them differently because of race, color, national origin, age, disability, sex, gender identity, or sexual orientation. Premera provides free aids and services to people with disabilities to communicate effectively with us, such as qualified sign language interpreters and written information in other formats (large print, audio, accessible electronic formats, other formats). Premera provides free language services to people whose primary language is not English, such as qualified interpreters and information written in other languages. If you need these services, contact the Civil Rights Coordinator. If you believe that Premera has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, sex, gender identity, or sexual orientation, you can file a grievance with: Civil Rights Coordinator — Complaints and Appeals, PO Box 91102, Seattle, WA 98111, Toll free: 855-332-4535, Fax: 425-918-5592, TTY: 711, Email AppealsDepartmentInquiries@Premera.com. You can file a grievance in person or by mail, fax, or email. If you need help filing a grievance, the Civil Rights Coordinator is available to help you. You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, electronically through the Office for Civil Rights Complaint Portal, available at <https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>, or by mail or phone at: U.S. Department of Health and Human Services, 200 Independence Ave SW, Room 509F, HHH Building, Washington, D.C. 20201, 1-800-368-1019, 800-537-7697 (TDD). Complaint forms are available at <http://www.hhs.gov/ocr/office/file/index.html>. You can also file a civil rights complaint with the Washington State Office of the Insurance Commissioner, electronically through the Office of the Insurance Commissioner Complaint Portal available at <https://www.insurance.wa.gov/file-complaint-or-check-your-complaint-status>, or by phone at 800-562-6900, 360-586-0241 (TDD). Complaint forms are available at <https://fortress.wa.gov/oic/onlineServices/cc/pub/complaintinformation.aspx>.

Language Assistance

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 800-722-1471 (TTY: 711).

注意: 如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 800-722-1471 (TTY: 711)。

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 800-722-1471 (TTY: 711).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 800-722-1471 (TTY: 711) 번으로 전화해 주십시오.

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 800-722-1471 (телетайп: 711).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulung sa wika nang walang bayad. Tumawag sa 800-722-1471 (TTY: 711).

УВАГА! Якщо ви розмовляєте українською мовою, ви можете звернутися до безкоштовної служби мовної підтримки.

Телефонуйте за номером 800-722-1471 (телетайп: 711).

ប្រយ័ត្ន: បើសិនជាអ្នកនិយាយភាសាខ្មែរ, សេវាជំនួយភាសាដោយមិនគិតថ្លៃ គឺអាចមានសំរាប់អ្នក។ ចូរ ទូរស័ព្ទ 800-722-1471 (TTY: 711)។

注意事項: 日本語を話される場合、無料の言語支援をご利用いただけます。800-722-1471 (TTY: 711) まで、お電話にてご連絡ください。

ማሳሰቢያ: የሚናገሩት ቋንቋ አማርኛ ከሆነ የትርጉም አርዳታ ድርጅቶች በነጻ ሊያገለግሉት ተዘጋጅተዋል፡ ወደ ሚከተለው ቁጥር ይደውሉ፡ 800-722-1471 (መስማት ለተሳናቸው: 711)፡

XIYEEFFANNAA: Afaan dubbattu Oroomiffa, tajaajila gargaarsa afaanii, kanfaltiidhaan ala, ni argama. Bilbilaa 800-722-1471 (TTY: 711).

ملحوظة: إذا كنت تتحدث انكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 800-722-1471 (رقم هاتف الصم والبكم: 711).

ਪਿਆਰ ਦਿਓ: ਜੇ ਤੁਸੀਂ ਪੰਜਾਬੀ ਬੋਲਦੇ ਹੋ, ਤਾਂ ਭਾਸ਼ਾ ਵਿੱਚ ਸਹਾਇਤਾ ਸੇਵਾ ਤੁਹਾਡੇ ਲਈ ਮੁਫਤ ਉਪਲਬਧ ਹੈ। 800-722-1471 (TTY: 711) 'ਤੇ ਕਾਲ ਕਰੋ।

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 800-722-1471 (TTY: 711).

ໂປດຊາບ: ຖ້າວ່າ ທ່ານເວົ້າພາສາ ລາວ, ການບໍລິການຊ່ວຍເຫຼືອດ້ານພາສາ, ໂດຍບໍ່ເສັຽຄ່າ, ແມ່ນມີພ້ອມໃຫ້ທ່ານ. ໂທ 800-722-1471 (TTY: 711).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 800-722-1471 (TTY: 711).

ATTENTION: Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 800-722-1471 (ATS: 711).

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 800-722-1471 (TTY: 711).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 800-722-1471 (TTY: 711).

ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 800-722-1471 (TTY: 711).

توجه: اگر بہ زبان فارسی گفتگو می کنید، تسهیلات زبانی بصورت رایگان برای شما فراهم می باشد. با 800-722-1471 (TTY: 711) تماس بگیرید.

