

Express Scripts
One Express Way, HQ2E03
St. Louis, MO 63121



March 18, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Reference Number: 3037100

Dear Attorney General,

I am writing to notify you of an incident impacting one Maryland resident that is a part of Express Scripts Pharmacy Benefit Management plan. Express Scripts identified a “credential stuffing” attack on February 21, 2022. The bad actor was able to log in to the member’s web account by reusing the member’s user ID and password likely obtained from another large public data breach (e.g. Yahoo, LinkedIn, etc.).

Possible data points viewed include name, address, date of birth, member ID, medication name, pharmacy name, and claim information. Express Scripts immediately locked the member’s account and required the member to call to reactivate the account. Additional monitoring is in place to detect and respond to any malicious activity. Blocking and preventative controls are also being implemented, including multi-factor authentication (MFA) later this year.

Please direct any inquiries regarding this matter to Laurie Wersching, Compliance Associate, at 800-332-5455 x346986. You may also contact the Privacy Office at Express Scripts, Inc., Mail Stop HQ2E03, One Express Way, St. Louis, MO 63121, or email us at Privacy@Express-Scripts.com. Please reference the following number when contacting the Privacy Office: 3037100.

Sincerely,

A handwritten signature in black ink that reads 'Kim Piant'.

Kimberly J. Piant
U.S. Privacy Officer
Express Scripts

Express Scripts
One Express Way, HQ2E03
St. Louis, MO 63121



DATE

NAME
ADDRESS
CITY, STATE ZIP

Re: **Express Scripts' Reference Number: 3037100**

Dear NAME:

Express Scripts is a business associate of <CLIENT> that handles prescription benefits. This letter serves to notify you of a potential compromise of your personally identifiable information (PII) and protected health information (PHI), as it is essential that <CLIENT> beneficiaries remain aware of any events that may affect their privacy.

The potential compromise occurred on February 21, 2022, when during internal system monitoring, Express Scripts identified potential unauthorized access to your Express Scripts web account. A login using the correct user ID and password occurred and was identified as suspicious on February 21, 2022. If this login was you, no disclosure of your information occurred. However, if the login was not you, during this access the individual may have viewed your name, address, date of birth, Express Scripts member identification number, claim information, names of physicians, names of pharmacies, medication names, and prescription numbers.

Express Scripts and its Privacy Office have thoroughly investigated the circumstances surrounding this situation, have determine the impact to be very limited and have taken steps to help mitigate any harm that might result from the disclosure. To prevent this from happening again, Express Scripts has locked your web account. Additional account monitoring is also in place. In order for a new account to be created, you will have to contact Express Scripts, making sure to use a different password when creating the new account. We also suggest you change your password on any other accounts where you may have used those same login credentials to protect your information.

At this time, we have no evidence to indicate you are at risk of identity theft and we believe there is little risk of exposure to fraud, but we desire to provide you with constructive assistance. Therefore, please be guided by the actions recommended by the Federal Trade Commission (FTC) which can be found at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm. The FTC website provides information on protecting your identity against fraud and instructions on placing a free fraud alert on your credit for a period of 90 days. Additionally, the site provides other valuable information regarding actions that can be taken now or in the future, should any problems develop.

We take this potential compromise very seriously. We value our beneficiaries and share the goal of safeguarding your information. On behalf of Express Scripts, I apologize for any inconvenience or concern this issue may have caused you. We look forward to continuing to provide services to you. If you have further questions or concerns, please contact Cheryl Starck, Sr. Compliance Analyst, at 314-684-6394. You may also contact the Privacy Office at Express Scripts, Mail Stop HQ2E03, One Express Way, St. Louis, MO 63121, or email us at Privacy@express-scripts.com. Please reference the following number when contacting the Privacy Office: 3037100.

Sincerely,

A handwritten signature in black ink that reads 'Kim Piant'.

Kimberly J. Piant
U.S. Privacy Officer
Express Scripts



April 20, 2022

Subject: Notification of Disclosure (3037100)

Dear _____ :

This letter is a follow up to our March 11, 2022 letter wherein we notified you of a potential compromise of your personally identifiable information (PII) and protected health information (PHI).

The potential compromise occurred on February 21, 2022, when during internal system monitoring, Express Scripts identified potential unauthorized access to your Express Scripts web account. A login using the correct user ID and password occurred and was identified as suspicious on February 21, 2022. If this login was you, no disclosure of your information occurred. However, if the login was not you, during this access the individual may have viewed your name, address, date of birth, Express Scripts member identification number, claims information, names of physicians, names of pharmacies, medication names, and prescription numbers.

Express Scripts and its Privacy Office have thoroughly investigated the circumstances surrounding this situation, have determined the impact to be very limited and have taken steps to help mitigate any harm that might result from the disclosure. To prevent this from happening again, Express Scripts has locked your web account. Additional account monitoring is also in place. In order for a new account to be created, you will have to contact Express Scripts, making sure to use a different password when creating the new account. We also suggest you change your password on any other accounts where you may have used those same login credentials to protect your information.

At this time, we have no evidence to indicate you are at risk of identity theft and we believe there is little risk of exposure to fraud, but we desire to provide you with constructive assistance. Therefore, please be guided by the actions recommended by the Federal Trade Commission (FTC) which can be found at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtheft04.shtm. The FTC website (www.ftc.gov or (877) 438-4338) provides information on protecting your identity against fraud and instructions on placing a free fraud alert on your credit for a period of 90 days. Additionally, the site provides other valuable information regarding actions that can be taken now or in the future, should any problems develop.

You may find additional resources about the risk of identity theft at the following locations:

Office of the Attorney General
Consumer Protection Division
200 Saint Paul Place
Baltimore, Maryland 21202
1-888-743-0023
www.marylandattorneygeneral.gov

Equifax Credit Information Services, LLC
P.O. Box 740241, Atlanta, GA 30374
800-509-8495
www.equifax.com

TransUnion Consumer Relations
P.O. Box 2000, Chester, PA 19016-2000
800-680-7289
www.transunion.com

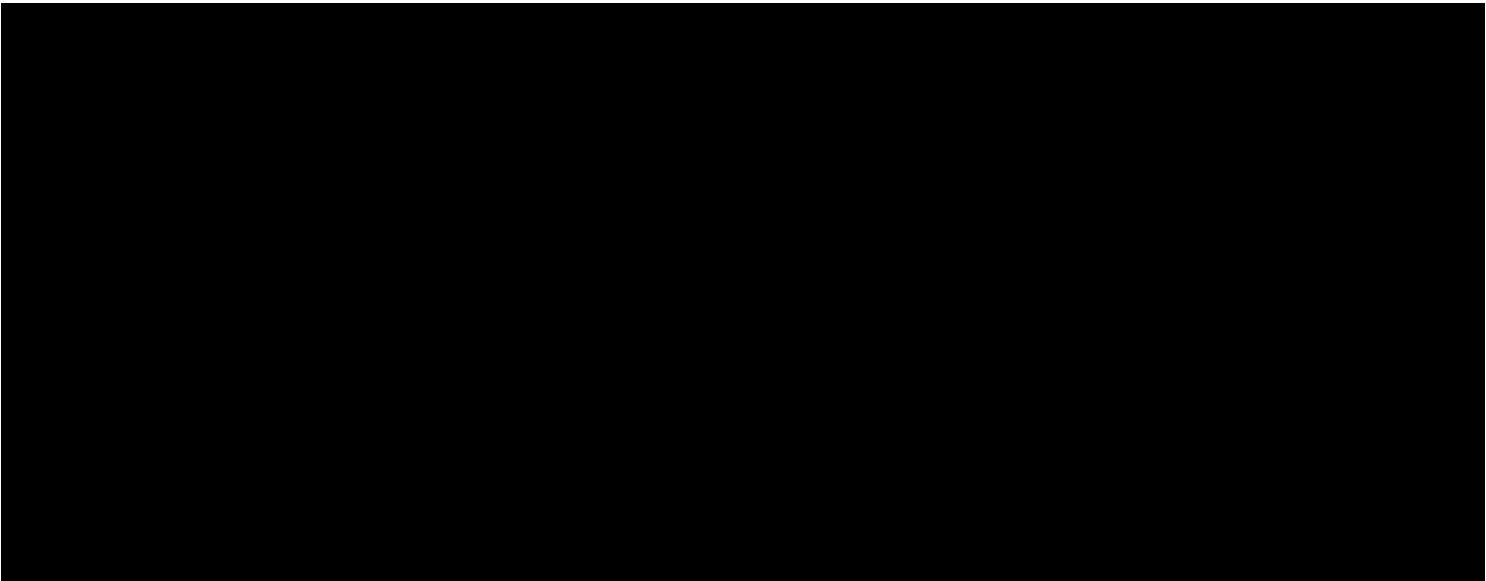
Experian National Consumer Assistance
Center
P.O. Box 4500, Allen, TX 75013
888-397-3742
www.experian.com

We take this potential compromise very seriously. We value our beneficiaries and share the goal of safeguarding your information. On behalf of Express Scripts, I apologize for any inconvenience or concern this issue may have caused you. We look forward to continuing to provide services to you. If you have further questions or concerns, please contact Cheryl Starck, Sr. Compliance Analyst, at 800-332-5455 x346394. You may also contact the Privacy Office at Express Scripts, Mail Stop HQ2E03, One Express Way, St. Louis, MO 63121, or email us at Privacy@express-scripts.com. Please reference the following number when contacting the Privacy Office: 3037100.

Sincerely,



Kimberly J. Piant
U.S. Privacy Officer
Express Scripts



Attached is the required notification related to a breach we were made aware of by one of our business associates.

Troy Lorents

Enterprise Privacy Office

tlorents@wlgore.com

T +1 928 864 2409 M +1 928 607 1344

W. L. Gore & Associates, Inc.

Together, improving life

1505 N. Fourth Street

Flagstaff, Az 86001

USA

gore.com

This email, including any attachment(s), contains information that may be confidential. This information is intended only for the use of the individuals or entities listed above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and destroy the original transmittal. If you have any questions, please see [Gore's Privacy Policy](#) or contact the privacy office at dataprivacyoffice@wlgore.com.



For information about our privacy practices, see our [Privacy Notice](#)

This email may contain trade secrets or privileged, undisclosed or otherwise confidential information. If you have received this email in error, you are hereby notified that any review, copying or distribution of it is strictly prohibited. Please inform us immediately and destroy the original transmittal. Thank you for your cooperation.

Client Breach Report

1. Breach Affecting:

- ☐ 500 or More Individuals
☒ Less Than 500 Individuals

2. Covered Entity Involved in Breach:

- a. Name of Covered Entity: W.L. Gore & Associates
- b. Address: 1505 N. Fourth Street
- c. Contact Name: Troy Lorents
- d. Contact Phone Number: 928.864.2409
- e. Contact E-mail: tlorents@wlgore.com
- f. Type of Covered Entity: Health Plan

3. Business Associate Involved in Breach:

- a. Name of Business Associate: Express Scripts, Inc.
- b. Address: One Express Way, HQ2E03, St. Louis, MO 63121
- c. Business Associate Contact Name: Kimberly J. Piant
- d. Business Associate Contact Phone Number: 314-692-1995
- e. Business Associate Contact E-mail: Privacy@express-scripts.com

4. Breach Start Date: 4/30/2022 Breach End Date: 5/1/2022

5. Discovery Start Date: 4/30/2022 Discovery End Date: 5/13/2022

6. Approximate Number of Individuals Affected by the Breach: varies by client

7. Type of Breach (check all that apply):

- ☐ Theft ☐ Loss

- | | |
|--|--|
| ☐ Improper Disposal | ☒ Unauthorized Access/Disclosure |
| ☐ Hacking/IT Incident | ☐ Unknown |

8. Location of Breached Information (check all that apply):

- | | |
|--|--|
| ☐ Laptop | ☐ Desktop Computer |
| ☐ Network Server | ☐ E-mail |
| ☐ Other Portable Electronic Device | ☐ Electronic Medical Record |
| ☐ Paper/Films | |
| ☒ Other (describe): <u>Express Scripts member mobile application</u> | |

9. Type of Protected Health Information Involved in the Breach (check all that apply):

- ☒ Demographic Information:
- ☒ Full Name ☐ DOB ☐ Address ☐ SSN ☐ Driver's License Number
- ☐ Other Identifier
- ☐ Financial Information:
- ☐ Account #/Credit Card # ☐ Claims Info. ☐ Other Financial Info.
- ☒ Clinical Information:
- ☐ Diagnosis/Conditions ☐ Lab Results ☒ Medications ☐ Other Treatment Information
- ☒ Other (e.g., name of physician, name of pharmacy): Name of pharmacy and prescribing physician, prescription number

10. Brief Description of the Breach: Based on proactive monitoring, Express Scripts, your Business Associate, identified a credential stuffing attack on April 30, 2022 in which user IDs and passwords compromised in other large public breaches were used by bad actors against the Express Scripts member application. The bad actor was able to log in to the member's web account by using the member's user ID and password made available after another public breach. Possible data points accessed include member name, medication name, prescription number, dosage, pharmacy name, prescriber name and prescriber contact information. Express Scripts locked the impacted member's account to prevent any further access, and the member will be required to reset their password. Additional monitoring, blocking, and preventative controls were implemented to detect and respond to malicious activity.

11. Safeguards in Place Prior to Breach (check all that apply):

- ☒ Privacy Rule Safeguards (Training, Policies and Procedures, etc.)



- ☒ Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
- ☒ Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
- ☒ Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

12. Actions Taken in Response to Breach (check all that apply):

- ☐ Adopted encryption technologies
- ☐ Changed password/strengthened password requirements
- ☐ Created a new/updated Security Rule Risk Management Plan
- ☒ Implemented new technical safeguards
- ☐ Implemented periodic technical and nontechnical evaluations
- ☐ Improved physical security
- ☐ Performed a new/updated Security Rule Risk Analysis
- ☐ Provided business associate with additional training on HIPAA requirements
- ☐ Provided individuals with free credit monitoring
- ☐ Revised business associate contracts
- ☐ Revised policies and procedures
- ☐ Sanctioned workforce members involved (including termination)
- ☒ Took steps to mitigate harm
- ☐ Trained or retrained workforce members
- ☐ Other (describe):

13. For report to HHS:

- a. Date(s) Individual Notice Provided (05/30/2022): Select date
- b. Was Substitute Notice Required?
☐ Yes ☒ No
- c. Was Media Notice Required?
☐ Yes ☒ No

14. Number of Individual Affected by the Breach.

4 Residents of Maryland