



May 27, 2022

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

Re: Notice of Cybersecurity Event

Dear Office of the Attorney General:

This letter is to inform you of a recent incident that involved the exposure of the Personal Information ("PI") and/or Protected Health Information ("PHI") of one (1) of your state's residents.

Highmark Inc., ("Highmark") is an independent licensee of the Blue Cross Blue Shield Association, headquartered in Pittsburgh, Pennsylvania. Highmark contracts with a vendor, Express Scripts, to provide pharmacy benefit services for Highmark and its affiliated entities.

The Highmark Privacy Department was notified on May 19, 2022 of a cybersecurity incident that occurred on the Express Scripts mobile application between April 30 and May 3, 2022. On April 30, 2022, through routine monitoring, Express Scripts identified an irregular volume of login attempts for the Express Scripts member mobile application. Upon identifying the suspicious activity, Express Scripts locked all potentially impacted accounts to prevent any further access, forced a password reset, and temporarily turned off the mobile application. Additional monitoring, blocking, and preventive controls were also put in place to detect and respond to any additional malicious activity.

Based on Express Scripts' investigation, it appears that the pattern of activity was indicative of a credential stuffing attack in which the threat actor obtains user ID and password information that was compromised in a prior unrelated event and tests those login credentials on another website or application, knowing that many individuals tend to reuse login information.

On May 13, 2022, after extensive forensic research, Express Scripts was able to positively identify those members whose accounts were potentially accessible to the threat actor. Express Scripts has provided us with information on the affected members and we were able to conclude on May 25, 2022 that this incident impacted one (1) Maryland resident.

While it appears that this was an automated attack to test the validity of the user account credentials, Express Scripts is unable to confirm whether or not information was actually viewed by the threat actor. The information that could have been accessed upon a successful login is 24 months of prescription information:

- Member name
- Medication name(s)
- Prescription number(s)
- Medication dosage
- Pharmacy name(s)
- Prescribing physician name and physician contact information

Please note that the unauthorized person(s) did not have access to social security numbers (SSN), full credit card numbers or financial information, date of birth or member ID number information.

Express Scripts and its Privacy Office have thoroughly investigated the circumstances surrounding this situation and have taken steps to help mitigate any harm that might result from the incident. Express Scripts has implemented a globally leading third-party security solution that monitors its applications 24x7 and detects and blocks bot activity targeting its mobile and web applications. In addition to deploying this additional fraud prevent control, Express Scripts has expedited plans to enforce mandatory multi-factor authentication. This matter was also reported to the Federal Bureau of Investigations Cyber Division on May 5, 2022.

Please be assured that this matter did not involve the Highmark network or systems in any way. As an additional precaution, Highmark has also locked the web account for these individuals, in the event these same login credentials are used to access our own member portal.

Highmark continues to work with Express Scripts to provide notice to all impacted parties and required state agencies. Each notice will contain an offer of complimentary identity theft protection services for a period of two years.

We regret this incident and want to assure you that Highmark takes the privacy and security of personal information very seriously. If you have any questions or concerns regarding this matter, please do not hesitate to contact me directly at 1-866-228-9424 or via email at Jill.Rosengren@highmarkhealth.org or privacy@highmark.com.

Sincerely,

Jill Rosengren

Jill Rosengren, JD, CIPP/US, CIPM
Director, Privacy and Data Ethics, Highmark Health Plans

JILL ROSENGREN
HIGHMARK
120 FIFTH AVENUE PLACE
2114
PITTSBURGH, PA 15222



PFAM147K000095 PF1M

SECURITY BREACH NOTIFICATION
OFFICE OF THE ATTORNEY GENERAL
200 ST. PAUL PLACE
BALTIMORE MD 21202



