NOTICE

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

Re: Notice Regarding Security Incident

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 some of your state's residents. Thirty-nine (39) residents of Maryland had information exposed that would trigger state data breach requirements.

Highmark Health is an independent licensee of the Blue Cross Blue Shield Association, headquartered in Pittsburgh, Pennsylvania. Highmark contracts with a third-party vendor, Webb Mason, who subcontracts to other vendors. One of those subcontractors, Quantum Group, has provided Webb Mason notice of a data security incident.

According to Quantum's notification to Webb Mason, which was received on December 28, 2021, Quantum experienced a cyber incident resulting in an unauthorized access to its network between August 17 and October 11, 2021. In response to this event, Quantum immediately initiated incident response protocols and began an investigation into the incident, engaged a third-party computer forensics firm, secured the compromised system, completed a global password reset, rebuilt the compromised server, deployed an endpoint detection and response system, and reported the matter to law enforcement.

Review of the affected files by Webb Mason determined that they contained information related to Highmark members. On January 14, 2022, Highmark learned of the impacted members and that the impacted files included data that was provided to Quantum in 2017 as part of the services performed by Webb Mason on behalf of Highmark. The information contained within the affected files was identified as having been related to a provider mailing regarding prescription drug changes which included member name, date of birth, health insurance identification number, and prescription information.

Since receiving notice of the Quantum breach from Webb Mason, Highmark has been diligently working to identify all impacted individuals to provide notice to individuals and required state agencies. Please be assured that this matter did not involve Highmark's network or systems in any way.

Individual notices will be sent to state residents via U.S. mail on or about March 10, 2022. Each notice will contain an offer of complimentary access to credit monitoring, fraud consultation, and identity theft restoration for a period of 12 months. Additionally, Highmark as committed to providing enhanced fraud monitoring to member accounts to examine it for any potential unauthorized use.

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 L. Rosengren, JD, CIPP/US
Director, Privacy and Data Ethics, Highmark Health Plans
jill.rosengren@highmarkhealth.org

Enclosure:

Individual Notice Template

WEBBMASON MARKETING

CORPORATE HEADQUARTERS
10830 Gilroy Road
Hunt Valley, Maryland 21031
410.785.1111 | f 410.584.7777

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

<<Date>>

Dear <<Full Name>>:

We are writing to inform you of a security incident experienced by Quantum Group ("Quantum") that may have involved your information as described below. We take the security and privacy of all information seriously and; therefore, it is crucial that we communicate with you and provide appropriate resources.

What happened?

WebbMason is a third-party vendor engaged by Highmark to provide marketing services. As part of these services, WebbMason engaged Quantum Group to provide printing and mailing services. On December 28, 2021, we received notification of a data security incident experienced by Quantum. According to Quantum's notification to us, Quantum experienced a cyber incident that resulted in unauthorized access to its network between **August 17 and October 11, 2021,** by an outside bad actor. Quantum immediately initiated incident response protocols and began an investigation into the incident. They also engaged a third-party computer forensics firm to assist in determining the cause and scope of the incident. Quantum's investigation determined that the unauthorized access to its network resulted in acquisition of certain files. Quantum subsequently performed a review of the impacted information to identify the types of information potentially impacted and to whom the information relates.

What information was involved?

On January 12, 2022, we learned that the impacted files included data provided to Quantum in 2017 as part of the services performed by WebbMason on behalf of Highmark. A further review of the affected files discovered that they contained information related to Highmark members. Please be assured that this matter did not involve Highmark's or WebbMason's network or systems in any way. The information contained within the affected files was identified as having been related to a provider mailing regarding prescription drug changes which includes your name, **Highmark member ID, date of birth, and prescription information.** Please be aware that your Social Security Number (SSN) was **not** accessed or acquired as part of this event.

What we are doing:

Quantum has assured us that they have taken the necessary steps to address this incident and to reinforce its existing security protocols and processes to reduce the likelihood of this situation occurring in the future. They immediately secured the compromised system, completed a global password reset, and blocked all remote activity to their network. Quantum has, since discovering the incident, rebuilt the compromised server and deployed an endpoint detection and response program that provides enhance network protection and monitoring. This matter was also reported to law enforcement.

Highmark has requested that Webb Mason discontinue using Quantum as a supplier for Highmark projects. Highmark will also provide enhanced fraud monitoring of your account to examine it for any unauthorized use.

While, at this time, we have no indication that your information has been misused, we have arranged for you to enroll, at no cost to you, in an online identity monitoring service for 12 months provided by Equifax. Additional information regarding

WEBBMASON MARKETING

CORPORATE HEADQUARTERS

10830 Gilroy Road
Hunt Valley, Maryland 21031
410.785.1111 | f 410.584.7777

how to enroll in the complimentary identity monitoring service is enclosed and will be available beginning on the date of this notice.

What you can do:

We recommend that you remain vigilant in regularly reviewing and monitoring all your accounts and explanation of benefits statements to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have also enclosed additional information about steps you can take to help protect yourself against fraud and identity theft.

Scams can be presented in multiple forms. You can take precautions to protect your information by being cautious of any unsolicited phone calls, mailings, or online activity. Do not give or send any personal information to people or businesses you don't know. You can protect your online activity by making sure that your computer security software is up to date and being careful about what links you click or items you download. If you are ever unsure or feel uneasy about a request for your personal information, it's best to not share any information at all.

For more information:

Should you have any questions or concerns regarding this incident, please reach out to our dedicated assistance line at 855-604-1883, Monday through Friday, (except U.S. holidays), from 9 a.m. – 9 p.m., EST. You may also contact Webb Mason by mail at 10830 Gilroy Rd., Hunt Valley, MD 21031. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Lynn M. Brewton
Chief Compliance Officer