Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 15, 2024

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Harvard Pilgrim Health Care ("Harvard Pilgrim") located at 1 Wellness Way, Canton, MA 02021 and write to supplement our June 15, 2023, July 20, 2023, and August 25, 2023 notices. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Harvard Pilgrim does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

On April 17, 2023, Harvard Pilgrim discovered it was the victim of a cybersecurity ransomware incident that impacted systems used to service members, accounts, brokers and providers. After detecting the unauthorized party, Harvard Pilgrim proactively took its systems offline to contain the threat. Harvard Pilgrim notified law enforcement and regulators and worked with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.

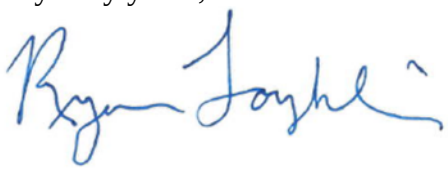
Harvard Pilgrim is continuing its active investigation. Unfortunately, the investigation identified signs that data was copied and taken from Harvard Pilgrim systems from March 28, 2023 to April 17, 2023. Harvard Pilgrim determined that the files at issue may contain personal information and/or protected health information. On May 23, 2023, Harvard Pilgrim began notifying potentially impacted individuals by posting notice to its website, providing notice to statewide media in all fifty (50) states and notifying providers, brokers and employer groups. On June 15,

2023, Harvard Pilgrim began providing written notice of this incident to individuals identified through its investigation.

Harvard Pilgrim's continued investigation revealed that the following information related to certain Harvard Pilgrim brokers and providers could potentially be in the files at issue: names and Social Security numbers. On February 15, 2024, Harvard Pilgrim continued to provide written notice of the incident to approximately one thousand thirty-nine (1,039) additional Iowa residents for whom it believes it had valid mailing address information. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/kzf
Enclosure

EXHIBIT A

Harvard Pilgrim Health Care

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/HPHC

February 15, 2024

Notice of <<Security Incident / Data Breach>>

Dear <<First Name>> <<Last Name>>,

Harvard Pilgrim Health Care ("Harvard Pilgrim") is writing to inform you of a cybersecurity incident that may involve your personal information. We are providing information about the measures Harvard Pilgrim has taken in response to the incident, and steps you can take to help protect yourself against possible misuse of information. You may have already received a similar letter if you have been a member of a Harvard Pilgrim health plan.

What Happened

On April 17, 2023, Harvard Pilgrim discovered it was the victim of a cybersecurity ransomware incident that impacted systems used to service members, accounts, brokers and providers. After detecting the unauthorized party, we proactively took our systems offline to contain the threat. We notified law enforcement and regulators and are working with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.

We take the privacy and security of the data entrusted to us seriously. Unfortunately, the investigation identified signs that data was copied and taken from Harvard Pilgrim systems from March 28, 2023, to April 17, 2023. On January 4, 2024, we determined that the files at issue may contain your personal information.

What Information Was Involved

The personal information in the files at issue may include your <<Variable Data: Data Elements>>. Harvard Pilgrim is not aware of any misuse of your personal information as a result of this incident.

What We Are Doing

As explained above, Harvard Pilgrim took immediate steps to secure its systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we implemented additional cybersecurity safeguards to our existing robust infrastructure to better minimize the likelihood of this type of event occurring again.

What You Can Do

We recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and to law enforcement. You may also review the guidance contained in *Steps You Can Take to Protect Personal Information.*

Additionally, Harvard Pilgrim is providing you with the opportunity to register for two (2) years of complimentary credit monitoring and identity protection services through IDX. Although we are making these services available to you, we are unable to enroll you directly. For enrollment instructions, please review the information contained in the attached *Steps You Can Take to Protect Personal Information*. If you are already enrolled in the complimentary credit monitoring and identity protection services provided, you do not need to enroll again.

For More Information

The security of your personal information is a top priority for us. We sincerely regret this incident occurred and for any concern it may cause you. We understand that you may have additional questions. For assistance with questions regarding this incident, please call IDX at (888) 693-0709 or go to https://response.idx.us/HPHC. Representatives are available between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday (excluding U.S. holidays).

Sincerely,

Christopher Walsh
VP, Privacy & Fraud Prevention and Recovery
Point32Health

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Enrollment Code: <<Enrollment Code>>

Go to https://response.idx.us/HPHC and follow the instructions for enrollment using your Enrollment Code above. Additionally, you may call the IDX call center at (888) 693-0709 (toll free), Monday through Friday from 9:00 a.m. to 9:00 p.m. ET, excluding U.S. holidays. Please note the deadline to enroll is May 15, 2024.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For California Residents, you can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa Residents, you may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office
Director of Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319
Phone: 1-515-281-5926
Website: www.iowattorneygeneral.gov

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, state laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Department of Justice at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
Phone: 1-877-877-9392
Website: www.doj.state.or.us

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 1347 Rhode Island residents that may be impacted by this event.