June 23, 2023

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

We are writing to notify you of a data security incident 72 New Hampshire residents.

IDENTIFICATION OF PARTIES

Point32Health, a sub-contractor of Health Plans, Inc. (HPI), and which is also the parent company of Harvard Pilgrim Health Care, experienced a ransomware incident in which the personal information of employees of Workers Federal Credit Union ("Workers" or the "Credit Union"), and their dependents, who are subscribers of HPI, was accessed by unauthorized parties. HPI is Workers health insurance vendor providing coverage to employees and their dependents. Point32Health is a vendor of HPI. In addition, employees of the Credit Union and their dependents may also be members of the Credit Union.

Personal information for employees and dependents of the Credit Union was maintained by Point32Health in their data systems, on behalf of HPI. Point32Health reported the incident to Workers on May 25, 2023. A copy of the notification Workers received from Point32Health is included with this notification.

NATURE OF THE DATA SECURITY INCIDENT

Workers received a notification email from Christopher Walsh, VP, Privacy & Fraud Prevention Recovery, with Point32Health, 1 Wellness Way, Canton, MA 02021, on May 25, 2023. The notification stated that Point32Health identified a cybersecurity ransomware incident in which data was copied and taken from their systems between March 28 and April 17, 2023.

Point32Health stated that they determined that the files at issue may contain personal information and/or protected health information for current and former HPI subscribers and dependents. Their investigation revealed that the following information could potentially be in the files at issue:

Point32Health informed Workers that they are not aware of any misuse of the personal information or protected health information as a result of this incident. Workers is also not aware of any misuse of our employees or dependents information as a result of the Point32Health incident.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The number of affected individuals (Workers employees and their dependents) residing in New Hampshire whose personal information was the subject of the incident, as known at the time of this notification, is 72. These New Hampshire residents will receive notice from Point32Health, which began mailing notices on behalf of Workers to each resident, starting on June 15, 2023. A copy of the notice is included for your reference.

STEPS TAKEN OR TO BE TAKEN RELATING TO THE INCIDENT

Upon notification by Point32Health of this incident, Workers Human Resources department notified all affected employees of the incident. The notification to employees included details regarding credit monitoring services being provided by Point32Health at their expense to all affected Workers employees and dependents, for a two-year period, and a telephone number to contact Point32Health with questions and requests for assistance.

The incident was reported internally to the Workers Risk Management Department and Information Security personnel. Workers initiated its Incident Response Team and began taking appropriate incident response steps. Workers Board of Directors was also notified.

Point32Health informed us that they took the affected systems offline, notified law enforcement, and began their investigation into the incident. The notification from Point32Health to Workers also described measures they are taken to enhance their security tools and procedures to prevent a similar incident from occurring.

CREDIT MONITORING SERVICES

Point32Health is offering immediate access to of complimentary credit monitoring and identity protection services through IDX to affected subscribers (employees and dependents). Instructions for obtaining this service were provided to affected employees on May 25, 2023 by Workers Human Resources department, and were also included in the Point32Health notification mailed to subscribers (employees and dependents).

If you have any questions or need further information, please contact me at your convenience.

Sincerely,

Patricia North-Martino
VP, Senior Information Security Risk Officer

Enclosures:

1. Point32Health Notification to Workers
2. Point32Health Notification to Subscribers

Harvard Pilgrim Health Care

Return to IDX
PO Box 480149
Niles, IL 60714

F 14878 T49 P1 3 **********AUTO**5-DIGIT 01532

To Enroll, Please Call:
(888) 220-5517
Or Visit:
https://response.idx.us/HPHC
Enrollment Code:

June 15, 2023

Dear

Harvard Pilgrim Health Care ("Harvard Pilgrim") is writing to inform you of a cybersecurity incident that may involve your personal information and/or protected health information. We are not aware of any misuse of your personal information or protected health information as a result of this incident. 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.

What Happened

Harvard Pilgrim is a subcontractor of Health Plans, Inc. ("HPI"), and we provide services to support the administration of health plans offered by HPI, which includes claims pricing, provider eligibility validation, and fraud, waste, and abuse analysis. On April 17, 2023, Harvard Pilgrim discovered it was the victim of a cybersecurity ransomware incident that impacted systems used to service clients, including HPI. 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. We are continuing our active investigation and conducting extensive system reviews and analysis before we can resume our normal business operations. Unfortunately, the investigation identified signs that data was copied and taken from Harvard Pilgrim systems from March 28, 2023, to April 17, 2023. On May 17, 2023, we determined that the files at issue may contain HPI personal information and/or protected health information.

What Information Was Involved

The personal information and/or protected health information in the files at issue may include:

Harvard Pilgrim is not aware of any misuse of your personal information or protected health 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 and/or are continuing to implement 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 explanations of benefits, 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 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 protected health 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 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: LC9X9LMSPD

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) 220-5517 (toll free), Monday through Friday from 9:00 a.m. to 9:00 p.m. ET, excluding U.S. holidays. If you are already enrolled in the complimentary credit monitoring and identity protection services provided, you do not need to enroll again. Please note the deadline to enroll is November 23, 2023.

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

Point32Health

Dear Health Plan's, Inc., Client:

On behalf of Health Plans, Inc., ("HPI"), Point32Health is writing to notify you of a data security incident that impacted our systems and may have resulted in the unauthorized access of your members' personal and/or protected health information. We are not aware of any misuse of the personal information or protected health information as a result of this incident.

Point32Health, a subcontracting business associate of HPI, provides services to HPI to support the administration of health plans offered by HPI, which include claims pricing for Harvard Pilgrim provider networks, provider eligibility validation, and fraud, waste, and abuse analysis. On April 17, 2023, Point32Health, the parent organization of Harvard Pilgrim Health Care and Tufts Health Plan, identified a cybersecurity ransomware incident that impacted Point32Health's systems. Upon discovering the unauthorized party, Point32Health proactively took their systems offline to contain the threat and notified law enforcement and regulators. Additionally, Point32Health promptly engaged with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.

Unfortunately, the investigation identified signs that data was copied and taken from Point32Health's systems between March 28, 2023, and April 17, 2023. On May 17, 2023, Point32Health determined that the files at issue may contain personal information and/or protected health information for current and former HPI subscribers and dependents. The investigation revealed that the following information related to your members could potentially be in the files at issue:

We are not aware of any misuse of the personal information or protected health information as a result of this incident.

Point32Health takes the privacy and security of the data entrusted to it seriously. Point32Health is continuing their active investigation and conducting extensive system reviews and analysis. In an effort to prevent a similar type of incident from occurring in the future, Point32Health: i) enhanced its security tools used to scan its networks for malware; (ii) is reviewing and enhancing user access protocols; (iii) is enhancing vulnerability scanning and prioritizing security improvements; (iv) is implementing a new sustainable Endpoint Detection and Response (EDR) security solution to detect and respond to cyber threats; (v) is conducting password resets for administrative accounts; and vi) is rebuilding or restoring its systems.

Point32Health plans to notify the affected health plan members and appropriate state and federal regulators and consumer reporting agencies of this incident on your behalf within the required statutory timeframes. The letter Point32Health proposes to send to potentially affected individuals affiliated with your group health plan, including a description of complimentary credit monitoring and identity protection services being offered, is attached as **Exhibit A** and **Exhibit B**. If you do not want Point32Health to perform these notifications on your behalf, please notify your Account Manager at HPI by Thursday, June 1, 2023.

In addition, Point32Health is also offering to provide your HPI subscribers and dependents with immediate access to two (2) years of complimentary credit monitoring and identity protection services through IDX. Although, Point32Health is making the credit monitoring and identity protection services available to members, we are unable to enroll them directly. Individuals may enroll by visiting and providing the following code: [redacted] or for minor dependents: [redacted] or calling for assistance. Representatives are available between the hours of 9:00

am to 9:00 pm Eastern time, Monday through Friday (excluding U.S. holidays).

If members have any questions about other issues unrelated to this ransomware incident or are being denied care, please have them call the number on the back of their member ID card for assistance. The notification to impacted individuals will include these instructions; however, we recommend you inform your health plan members of these services earlier via your company intranet, email, etc. We have attached a suggested communication as **Exhibit C**.

We understand you or your members may have questions regarding the incident. Please reach out to your HPI Account Manager for answers regarding the incident.

Point32Health is continuing to work with third-party cybersecurity experts to complete a thorough investigation into this incident and remediate the situation and will provide updates as we learn of information that impacts your membership.

We appreciate your patience and regret any inconvenience that this incident may have caused.

Sincerely,

Christopher Walsh
VP, Privacy & Fraud Prevention and Recovery
Point32Health