Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
100 Crescent Court, Suite 700
Dallas, Texas 75201
LFunk@constangy.com
Mobile: 248.709.9385

February 27, 2026

Via Postal Mail
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Tel: 206-464-6684

Re: Notification of Data Security Event

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents PIH Health, Inc. ("PIH Health") in connection with its response to a data security event discussed below. PIH Health is located at 12462 Putman Street, Whittier, California 90602. The purpose of this letter is to notify you of the event in accordance with Washington data breach notification statute. By providing this notice, PIH Health does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

1. Nature of the Security Event

On December 1, 2024, PIH Health became aware of unusual activity involving a portion of its environment. Upon becoming aware of this activity, it took immediate measures to secure the network and launched an investigation to evaluate what happened and determine if any sensitive or confidential information may have been affected as a result of the incident. The investigation concluded that certain information was accessed by an unauthorized actor. Subsequently, with the assistance of third-party specialists, PIH Health undertook a detailed and time-intensive review of all affected data to identify whether any individual information was contained therein and confirmed on or around December 16, 2025, the presence of personal information. Following this discovery, PIH Health worked to gather contact information needed to provide notification. This process concluded on February 25, 2026.

Please note that PIH Health has no evidence of any actual or suspected misuse of information involved in this incident.

2. Number of Affected Washington Residents & Information Involved

The event involved personal information for approximately 3,639 Washington residents and included name, Social Security number or individual taxpayer identification number, driver's license or state identification number, date of birth, medical information, and health insurance information.

3. Notification to Identified Individuals

On February 27, 2026, notification letters were sent to identified Washington residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services provided through Experian including 12 months of services. A sample notification letter is enclosed.

4. Measures Taken to Address the Event

Upon identifying this event, in addition to taking the steps described above, PIH Health took steps to learn more about what happened and what information could have been affected. PIH Health notified the identified individuals and provided them with steps they can take to protect their personal information, including providing them with information about its toll-free call center through to answer questions about the event, address-related concerns, and enrolling in the credit monitoring services.

PIH Health also notified the United States Department of Health and Human Services and applicable state regulatory authorities. PIH Health also provided notice of the event to the appropriate media outlets pursuant to the Health Insurance Portability and Accountability Act.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at LFunk@constangy.com.

Sincerely,

Laura Funk of
Constangy, Brooks, Smith & Prophete LLP

Encl.: Sample Notification Letter

14232164v1
14233116v1

Return Mail Processing
PO Box 999
Suwanee, GA 30024

117**********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 27, 2026

Subject: Notice of Data [Extra1]

Dear Sample A. Sample,

PIH Health, Inc. ("PIH Health") is writing to inform you of a data security incident that may have involved your information. We take the privacy and security of individual information very seriously. Please read this letter carefully as it contains additional details regarding the incident and steps you can take to help protect your information.

What Happened? On or about December 16, 2025, PIH Health confirmed the presence of personal information in files identified to have been accessed or acquired without authorization during a December 2024 incident. Specifically, on December 1, 2024, PIH Health discovered unusual activity within a portion of our digital environment. Upon becoming aware of this activity, we took measures to secure the network and launched an investigation to evaluate what happened and determine what information may have been affected as a result of the incident. The investigation concluded that certain information was accessed by an unauthorized actor. Subsequently, with the assistance of third-party specialists, PIH Health undertook a time intensive and detailed review of all potentially affected data to identify whether any individual information was contained therein. Following completion of that review, PIH Health confirmed that individual personal information was contained within the potentially affected data and worked to gather contact information needed to provide notification. This process was completed on February 25, 2026.

Please note, we have no evidence of the misuse, or attempted misuse, of any potentially affected information.

What Information Was Involved? The information identified during the review included your name and [Extra4][Extra5].

What We Are Doing. As soon as we became aware of the event, we took the steps described above and implemented additional security measures to help minimize the risk of a similar incident occurring in the future. We are also notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you the opportunity to enroll in complimentary identity protection services through Experian.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for [Extra3] months.
If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** June 30, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: http://www.experianidworks.com/3bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by June 30, 2026 at 1-833-918-8201 Monday through Friday from 6:00 AM to 6:00 PM PT (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do. Please review this letter carefully along with the recommendations on the following page to help protect your information. You can also enroll in the complimentary services offered to you through Experian by using the enrollment code provided above.

For More Information. If you have questions about this letter or need assistance, please call Experian at 1-833-918-8201. Experian representatives are available Monday through Friday from 6:00 AM to 6:00 PM PT, excluding United States holidays. Experian representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We take this event and the security of information in our care seriously. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

PIH Health, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
1-888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
1-877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
1-800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
www.ag.ny.gov
1-800-771-7755

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400
There were 174 Rhode Island Residents Impacted.

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
1-888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
1-212-416-8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
www.oag.dc.gov/consumer-protection
1-202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
1-502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov/protectingconsumers/
1-877-566-7226

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf