Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103

October 29, 2024

VIA U.S. MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Security Incident

To Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Soliant Health, LLC and its affiliate brands ("Soliant") in connection with a recent data security incident described below. Soliant is notifying affected individuals of the incident. The purpose of this letter is to provide formal notice to your office pursuant to N.H. Rev. Stat. § 359-C:20.

I. Nature of the Security Incident

On June 25, 2024, Soliant discovered suspicious activity associated with an employee's email account. Upon discovery, Soliant immediately took steps to address the issue and secure its email environment, including engaging a team of cybersecurity specialists, implementing a forced password reset, working with law enforcement, and launching a comprehensive investigation. The investigation determined that certain personal information may have been acquired without authorization. Soliant thereafter undertook a comprehensive review to determine the nature of the information, the individuals to whom the information pertained and the addresses for those individuals. That process was completed on October 3, 2024. Soliant thereafter worked diligently to arrange for notice and remediation services to the affected individuals.

II. Number of New Hampshire Residents Affected

Soliant's investigation determined that personal information for a total of seventeen (17) New Hampshire residents may have been involved. The potentially affected personal information for New Hampshire residents included

.

Notification letters were sent to these individuals via first class U.S. mail on October 29, 2024. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

III. Actions Taken in Response to the Incident

As soon as Soliant discovered the unusual network activity, it took immediate steps to secure its network, launched an investigation with the assistance of independent experts, and worked to determine whether any personal information was accessed or acquired without authorization in connection with the incident. Soliant thereafter worked diligently to determine what personal information may have been affected, the

individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

Soliant has established a toll-free call center through Epiq to answer questions about the incident and address related concerns. In addition, Soliant is offering New Hampshire residents whose Social Security numbers or driver's license information may have been affected twelve (12) months of complimentary credit and identity protection services through Experian IdentityWorks.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

Aubrey L. Weaver
Partner, Cybersecurity & Data Privacy Team

Encl. Sample Consumer Notification Letter

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Subject: Notice of Data <<Variable Data 1>>

Dear <<Full Name>>:

We are writing to inform you of a data security incident that may have involved your personal information. Soliant Health, LLC, and its affiliates ("Soliant") takes the privacy and security of the data under our care very seriously and we regret any concern or inconvenience this may cause. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On June 25, 2024, Soliant discovered suspicious activity associated with an employee's email account. Upon discovery, Soliant immediately took steps to address the issue and secure its email environment, including engaging a team of cybersecurity specialists, implementing a forced password reset, working with law enforcement, and launching a comprehensive investigation. The investigation determined that certain personal information may have been acquired without authorization. Soliant thereafter undertook a comprehensive review to determine the nature of the information, the individuals to whom the information pertained and the addresses for those individuals. That process was completed on October 3, 2024.

What Information Was Involved. The information may have included your <<Data Elements>>.

What We Are Doing. As soon as Soliant discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future.

As an additional resource to help protect your information, Soliant is offering individuals whose information was involved in this incident complimentary access to Experian IdentityWorks^{SM} for . If you believe there has been unauthorized use of your information and want 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 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 with contacting credit grantors to dispute charges and close accounts; assisting in placing a freeze on your credit file with the three major credit bureaus; and assisting with contacting government agencies to help restore your identity to its proper condition).

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

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

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or want an alternative to enrolling in Experian IdentityWorks online, contact Experian's customer care team at 877.288.8057 by Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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.[1]
- 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[2]: Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through Experian using the instructions provided in this letter.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 855-277-7578 Monday through Friday from 9 am to 9 pm ET. We take your trust in us and this matter very seriously.

Sincerely,

Soliant

[1] Offline members are eligible to call for additional reports quarterly after enrolling.

[2] 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 Personal 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 (the "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 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
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
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 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.

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.

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

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

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

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

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

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

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

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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

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

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

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.