Lindsay Nickle, Partner
1201 Elm Street, Suite 2550
Dallas, Texas 75270
lnickle@constangy.com
Direct: 806-535-0274

August 14, 2023

Via Electronic Submission

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notice of Data Security Incident**

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Sightpath Medical, LLC ("Sightpath"), a company based in Minneapolis, Minnesota, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maine data breach notification statute.

1. What Happened

On February 9, 2022, Sightpath discovered unusual activity in its digital environment. Upon discovering this activity, Sightpath immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. As a result of this investigation, Sightpath learned certain personal information may have been accessed or acquired without authorization during the incident. On or about June 14, 2023, Sightpath completed a comprehensive review of the impacted data potentially containing personal information through which Sightpath identified certain personal information as potentially involved. Sightpath then worked diligently to identify current contact information to issue notification to relevant individuals.

2. Number of Maine Residents Notified and Type of Information

On August 14, 2023, Sightpath notified one (1) Maine resident of this data security incident via U.S. First-Class Mail. The data sets potentially accessible by the malicious actor(s) responsible for this incident included name and Social Security number. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Sightpath reported this incident to law enforcement and will cooperate as necessary. It has also

implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Sightpath has offered notified individuals 12 months of complimentary services through Experian, which includes credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

4. Contact Information

Sightpath remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Best regards,

/s/ Lindsay Nickle

Lindsay Nickle
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

SIGHTPATH MEDICAL™
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 14, 2023

J8585-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Subject: Notice of Data Breach

Dear Sample A. Sample,

I am writing to inform you of a recent data security incident experienced by Sightpath Medical, LLC, ("Sightpath") that may have affected your personal information[1]. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? On February 9, 2022, Sightpath discovered unusual activity in our digital environment. We immediately took steps to secure our digital environment and engaged a dedicated team of external cybersecurity experts to assist us in responding to and investigating the incident. As a result of the investigation, we learned that an unauthorized actor accessed certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify the individuals and information involved. On June 14, 2023, we determined that personal information may have been involved in this incident. Since that time, we have worked to gather information necessary to meet reporting and notification obligations.

What Information Was Involved? The potentially affected information includes your name and [Extra1].

What Are We Doing? As soon as Sightpath discovered this incident, we took the steps described above. In addition, we have implemented additional measures to further enhance the security of our environment in the effort to minimize the risk of a similar incident occurring in the future.

Additionally, to help protect your information, we are offering complimentary access to Experian IdentityWorks^{SM} for ## 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).

[1] If you are receiving this letter then you are likely a current or former employee of Sightpath; or a beneficiary of an employee of Sightpath who listed your information as part of their employment benefits.

Please note that Identity Restoration is available to you for ## 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 <<12/24>>-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 November 30, 2023 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- 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 at 833-420-2825 by November 30, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do: We recommend you activate your complimentary Experian services using the information provided above. You can also follow the recommendations on the following page to help protect your personal information.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions about the incident, please call our dedicated call center at 833-420-2825 from Monday through Friday from 6:00 A.M. to 8:00 P.M. Pacific Time or Saturday through Sunday from 8:00 A.M. to 5:00 P.M. Pacific Time (excluding holidays). The call center representatives are fully versed on this incident and can answer questions that you may have.

Please be assured that Sightpath takes the privacy and security of all personal information within its possession very seriously. We hope you will accept our sincere apologies and know that Sightpath deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Charice Anderson

Charice Anderson, Chief Legal & Administrative Officer
Sightpath Medical, LLC
5775 W Old Shakopee Rd
Minneapolis, MN 55437

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
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 2000
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 http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. A security freeze will stay on your credit report until you remove it, and 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, and
www.ftc.gov/idtheft
1-877-438-4338

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

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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.

ADDITIONAL DETAILS REGARDING YOUR ##-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.